ANÁLISIS DE LOS PROTOCOLOS DE CONTROL DE INTEGRIDAD EXISTENTES EN REDES VANETS (Vehicular Ad-Hoc Networks)

CARLOS MAURICIO MUÑOZ EBRATT - T00014548

ROBERTO CARLOS ROMERO PAYARES - T00014997

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA D. T. Y C.

2010

ANÁLISIS DE LOS PROTOCOLOS CONTROL DE INTEGRIDAD EXISTENTES EN REDES VANETS (Vehicular Ad-Hoc Networks)

CARLOS MAURICIO MUÑOZ EBRATT - T00014548

ROBERTO CARLOS ROMERO PAYARES - T00014997

Monografía

Docente ISAAC ZÚÑIGA SILGADO

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA D. T. Y C.

2010

Nota de aceptación

_____

_____

_____

_____

Jurado

_____

_____

_____

_____

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no se pueden ser explotados comercialmente sin autorización.

DEDICATORIA

Gracias Dios por darme el privilegio de poder estudiar, así como también la sabiduría y madures para poder enfrentar cada uno de los retos que surgieron a lo largo del proceso.

Agradezco:

Muy especialmente a mi abuelo Luis Hernando Muñoz Roa, cuya voluntad fue la promotora de mis estudios universitarios.

A mi madre y mi novia por su comprensión, y mis abuelos por brindarme todas las oportunidades que me permitieron estudiar la carrera de ingeniería de sistemas en la mejor Universidad de Bolívar.

Así mismo, agradezco a nuestro tutor Isaac Zúñiga Silgado por su asesoramiento y apoyo brindado, quien ha hecho posible la culminación de nuestra monografía.

Agradezco igualmente a docentes y compañeros de carrera, amigos, familiares y demás quienes permitieron también que se lograra esta meta.

CARLOS MAURICIO MUÑOZ EBRATT

DEDICATORIA

A Dios por ser el pilar de mi vida y desarrollar en mí, habilidades y talentos que permitieron culminar mi carrera universitaria.

A mis padres: Roberto y Maritza por el apoyo incondicional, amor y entrega en cada paso de mi formación.

A Rafi, Chela, mi novia, familiares, amigos y compañeros de universidad por acompañarme y colaborarme en todo momento.

Gracias a la Universidad Tecnológica de Bolívar y al programa de Ingeniería de Sistemas por ser el escenario donde me forme como profesional y culminé todos mis objetivos.

Al cuerpo docente y en especial a nuestro tutor Isaac Zúñiga Silgado por sus conocimientos, aportes y colaboración en el desarrollo y finalización de este trabajo de grado.

ROBERTO CARLOS ROMERO PAYARES

AUTORIZACIÓN

Cartagena de Indias D. T. y C.

Nosotros CARLOS MAURICIO MUÑOZ EBRATT, con cédula de ciudadanía 1047.367.270 de Cartagena y ROBERTO CARLOS ROMERO PAYARES con cédula de ciudadanía 1.047.367.269, autorizamos a la Universidad Tecnológica de Bolívar para hacer uso de nuestro trabajo de grado y publicarlo en el catálogo online de la biblioteca.

Cordialmente,

CARLOS M. MUÑOZ EBRATT	ROBERTO C. ROMERO PAYARES
CC.1047.367.270 de Cartagena	CC. 1047.367.269 de Cartagena

Cartagena de Indias D. T. y C.

Señores

COMITÉ CURRICULAR
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
Ciudad

Respetados señores:

Por medio de la presente me permito hacer entrega de la monografía titulada **ANÁLISIS DE LOS PROTOCOLOS DE CONTROL DE INTEGRIDAD DE INFORMACIÓN EN REDES VANETS**, para su estudio y evaluación, la cual fue realizada por los estudiantes CARLOS MAURICIO MUÑOZ EBRATT y ROBERTO CARLOS ROMERO PAYARES y de la cual acepto ser su director.

Atentamente,

_____

ING. ISAAC ZÚÑIGA SILGADO

Cartagena de Indias D. T. y C.

Señores

COMITÉ CURRICULAR

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
Ciudad

Estimados Señores.

Con todo el interés me dirijo a Uds. Para presentar a su consideración, estudio y aprobación la monografía titulada **ANÁLISIS DE LOS PROTOCOLOS DE CONTROL DE INTEGRIDAD DE INFORMACIÓN EN REDES VANETS**, como requisito para obtener el título de Ingeniero de Sistemas.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios de la Universidad para los trabajos de grado.

Cordialmente,

CARLOS M. MUÑOZ EBRATT	ROBERTO C. ROMERO PAYARES
CC.1047.367.270 de Cartagena	CC. 1047.367.269 de Cartagena

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Desde sus inicios las redes VANETS han venido utilizando los mismos protocolos de las redes inalámbricas convencionales, debido la topología y al medio son vulnerables a ataques. Por esta razón la IEEE desarrollo un mecanismo conocido como WEP diseñado para proporcionar integridad en el tráfico de datos, siendo este vulnerado rápidamente en el vector de inicialización. Posteriormente la asociación de empresas Wi-Fi decidió lanzar un mecanismo de seguridad intermedia de transición llamado WPA, que es considerado el estándar recomendado. Dentro de las mejoras de WPA, surgió una extensión llamada WPA2 implementando otro algoritmo y soporte en los modos de funcionamiento. Finalmente TKIP ofrece mejoras significativas en la codificación de datos, el cual fue diseñado en gran medida para corregir las deficiencias de encriptación del protocolo WEP.

Las redes VANETS son redes inalámbricas de acceso vehicular. En esta monografía se analizarán principalmente cuatro protocolos nombrados anteriormente, los cuales hacen parte del contexto de la seguridad en redes inalámbricas y por tanto en redes vehiculares; esto con el fin de identificar los alcances e inconvenientes de los mismos. Para ello, se definirán las características de los protocolos de control de integridad, se identificaran los simuladores de red que permitan analizarlos, se harán simulaciones de estos protocolos y como resultado se generará una tabla comparativa del comportamiento de estos a fin de que se hagan notables sus características.

En la actualidad existe una problemática alrededor de la seguridad en la redes VANETS, dicha problemática es inherente a las características del medio de transmisión de los datos en este tipo de redes. El problema que se desea abordar, es el de la falta de seguridad para con la información en estas redes, la cual surge a partir de la necesidad de proteger la integridad de la información donde no existe una infraestructura tecnológica que permita evitar inclusiones al medio.

En este trabajo de monografía, inicialmente se revisará de manera cuidadosa la literatura más reciente acerca de las características de los protocolos de control de integridad, su funcionamiento y fallas en la seguridad. A fin de elegir una herramienta de simulación, se revisarán las herramientas más utilizadas para la simulación en redes, con el propósito de buscar aquellas que cumplan con los requerimientos para la mostrar la arquitectura de red en un escenario de redes VANETS. Posteriormente se realizará un ejercicio de crackeo del protocolo WEP y WPA con el fin de ilustrar la vulnerabilidad de los protocolos.

RESUMEN

En el ámbito de la seguridad de redes ad-hoc, más específicamente en redes vehiculares móviles (VANETS), existen un conjunto de consideraciones que se deben tener en cuenta para la implementación de redes de este tipo y que aseguren la integridad de la información que viaja a través de estas. Para tal efecto se implementan protocolos específicos que permitan asegurar dicha integridad, en algunos casos de una manera más eficaz que en otros.

Hay cuatro protocolos de control de integridad más populares que implementan diferentes mecanismos y de allí sus diferentes características. El primero es el WEP (Wired Equivalency Privacy) que se configura como uno de los primeros protocolos de encriptación introducido en el estándar IEEE 802.11 y el cual utilizaba el algoritmo RC4 para el cifrado de datos. Luego surge el WPA (Wireless Protected Access) como resultado de las fallas visibles en WEP, el cual solucionaba las debilidades conocidas de este anterior protocolo. Las características principales de este protocolo WPA eran entonces la utilización de un sistemas de encriptación mediante TKIP y autenticación mediante el estándar 802.11x. A pesar de los nuevos mecanismos implementados en este protocolo seguían existiendo algunas debilidades en él, debido a las características heredadas de WEP, por lo que en el 2004 fue lanzada una versión certificada que corregía estas debilidades, este protocolo era WPA2.

WPA2, haría parte del estándar IEEE802.11i, e implementaría algunos cambios y características. Al igual que WPA, este nuevo protocolo también utilizaba EAP para la autenticación, pero ahora se reemplazaba el algoritmo MICHAEL utilizado en WEP y WPA, por un código de autenticación CCMP, considerado criptográficamente seguro. Adicional, se reemplazaría el antiguo RC4 por un estándar avanzado de encriptación AES.

Por último el protocolo TKIP (Temporal Key Integrity Protocol), el cual es una mejora de protocolo WEP e implementa una mezcla de claves de sesión con un vector de inicialización en cada paquete. Este utiliza también el algoritmo de

cifrado RC4, sin embargo las llaves son de 128 bits para el cifrado y 64 bits para la autenticación, lo que resuelve el problema de longitud de clave corta que tenía WEP.

Por otro lado, hay herramientas que permiten el análisis de estos protocolos descritos, sea con fines académicos o de investigación. En cualquiera de los casos, estas herramientas que simulan escenarios reales, permiten un acercamiento y una visión más amplia del funcionamiento de ellos y que con los resultados y el análisis permitirían el diseño de una solución si fuera el caso.

La simulación es una técnica que busca imitar el comportamiento de un sistema real conforme evoluciona el tiempo, de manera que se puede hacer un análisis prescindiendo de un sistema netamente real. El crecimiento vertiginoso del desarrollo de tecnologías de comunicación hace necesario la utilización de estas herramientas que permite ser más eficaz al momento del diseño de una solución. Abaratar los costos de diseño, mejorar la calidad y reducir el tiempo de lanzamiento de un producto al mercado, son bondades de los simuladores.

En la actualidad, los simuladores de redes son herramientas ampliamente usadas en el mundo de la Ingeniería, puesto que permiten modelar redes de computadores completas definiendo los comportamientos específicos de sus nodos, dispositivos y enlaces en un escenario virtual con el que se puede interactuar. Para efectos de simulaciones en el área de la seguridad de redes, existen varios desarrolladores los cuales tienen distintas orientaciones y características. Algunos de ellos son OPNET, OMNET, NS2, NS3, QUANET.

Otras herramientas pueden ser utilizadas para el análisis de seguridad de las redes, como son las de sniff (monitoreo de red) y de crackeo. Estas permiten la captura de paquetes en redes alámbricas e inalámbricas permitiendo hacer un análisis más real de vulnerabilidades y fortalezas de los protocolos. Ejemplos de estas herramientas son COMMVIEW y AIRCRACK, que juntas se configuran como herramientas de crackeo de la seguridad de las redes y una opción para el rompimiento de la seguridad de las redes VANETS.

CAPÍTULO 1

PROTOCOLOS DE CONTROL DE INTEGRIDAD

1.1 **INTRODUCCIÓN**

La seguridad es un aspecto que cobra especial relevancia cuando se habla de redes de acceso vehicular debido a que la topología y el medio de comunicación son vulnerables. La integridad es uno de los atributos que conforma la seguridad, por esta razón en este capítulo se definirán las características de los protocolos pertinentes con el fin de evaluarlas en este ámbito. Estos protocolos que hacen parte de la seguridad en VANETS son: WEP, WPA, WPA2 y TKIP.

1.2 **WEP (Wired Equivalent Privacy)**

WEP fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 en el año 1999. Este, utiliza una misma clave simétrica y estática en las estaciones y en el punto de acceso. El estándar no contempla ningún mecanismo de distribución automático de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red lo que genera varios inconvenientes. Por un lado, la segunda clave está almacenada en todas las estaciones aumentando las posibilidades de que sea comprometida, y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva en la mayoría de las ocasiones, a que la clave se cambie poco o nunca. El algoritmo de encriptación utilizado es RC4 con claves de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. [1].

1.2.1 COMPONENTES DE WEP

WEP consta de cuatro componentes para su funcionamiento: una llave secreta, un vector de inicialización, el algoritmo RC4 y el CRC-32.

- Llave secreta
  La mayoría de los puntos de acceso utilizados en redes IEEE 802.11 utilizan llaves secretas estáticas que comparten con los usuarios de la red para iniciar transmisión de datos. Estas llaves se utilizan para encriptar información con el algoritmo RC4. Esta llave normalmente es de 40 bits aunque existen implementaciones que usan llaves de 104 bits con el fin de ofrecer un nivel mayor de seguridad.

- Vector de inicialización
  Es un vector de 24 bits que se añadirá a la clave WEP. El IV será diferente para cada trama que se cifre (representa la parte variable de la clave de cifrado). Sumando estos 24 bits a los proporcionados por la clave *WEP* tenemos que, para generar el *Key Stream RC4* se usan 64 (40 fijos más 24 variables) o 128 bits (104 fijos más 24 variables).

- Algoritmo RC4
  Es el algoritmo de cifrado de flujo más usado en la actualidad. Fue creado por Ron Rivest en 1987 y se mantuvo en secreto hasta 1994 cuando se hizo público. Los cifrados de flujo funcionan expandiendo una llave o cadena de bits, en una clave arbitrariamente larga de bits pseudo aleatorios. En el caso de WEP, la llave se forma por el vector de inicialización y la llave secreta compartida. Estas llaves alimentan al algoritmo RC4 para generar la secuencia de llaves utilizada para encriptar y desencriptar la información.

- CRC-32
  Para calcular las sumas de verificación se utilizan códigos de redundancia cíclica, también llamados códigos polinomios. Estos son muy utilizados para la detección de errores en largas secuencias de datos. Se basan en el uso de un polinomio generador utilizado en el proceso de encriptación y desencriptación de WEP. [1]

1.2.2 FUNCIONAMIENTO DE WEP

Proceso de encriptación

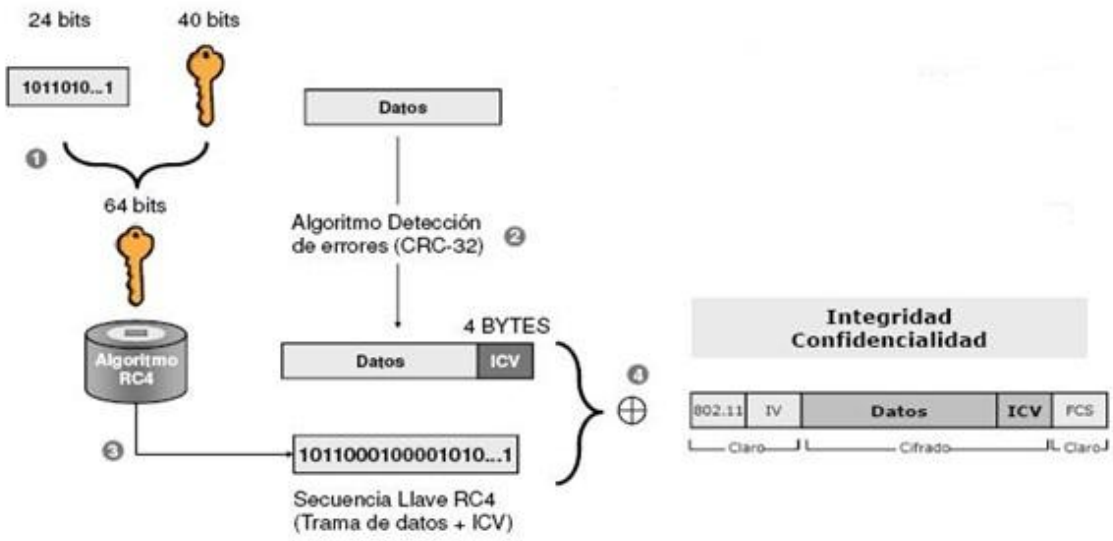


Fig. 1. Proceso de encriptación WEP.

a. La llave secreta de 40 bits se combina con un vector de inicialización de 24 bits para formar la llave RC4.
b. En paralelo, la trama de datos se protege con un vector de chequeo de integridad (CRC-32).
c. La llave se pasa por el algoritmo RC4, formando una secuencia de bits de longitud apropiada.
d. Esta secuencia se emplea para cifrar la información y el ICV (operación lógica XOR). [2]

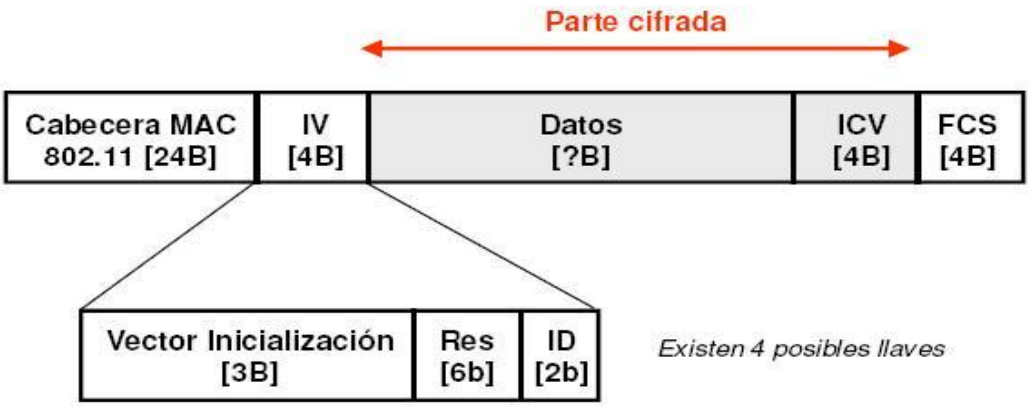


Fig. 2. Trama de datos WEP.

Proceso de desencriptación:

La desencriptación en el receptor se realiza para cada trama 802.11, este proceso se describe en los siguientes pasos:

- El receptor utiliza el IV enviado por el transmisor y la llave secreta compartida para generar una secuencia de llaves con el algoritmo RC4.
- El receptor realizar la operación XOR entre la secuencia de llaves y el texto cifrado recibido para calcular el texto original y el ICV.
- Con el CRC-32 se calcula el valor ICV del texto original ya obtenido.
- Si los valores ICV son iguales, acepta el mensaje, sino lo rechaza. [2]

1.2.3. FALLOS DE SEGURIDAD EN WEP

- Debilidades del algoritmo RC4 dentro del protocolo WEP debido a la construcción de la clave.

- Los IVs son demasiado cortos (24 bits – hacen falta menos de 5000 paquetes para tener un 50% de posibilidades de dar con la clave), y se permite la reutilización de IV (no hay protección contra la repetición de mensajes).

- No existe una comprobación de integridad apropiada (se utiliza CRC32 para la detección de errores y no es criptográficamente seguro por su linealidad).

- No existe un método integrado de actualización de las claves. [3]

El principal problema radica en que no implementa adecuadamente el vector de iniciación del algoritmo RC4, debido a que utiliza un enfoque directo y predecible para incrementar el vector de un paquete a otro. Además existe un problema con el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación. Conociendo los IV utilizados repetidamente y aplicando técnicas relativamente simples de descifrado puede finalmente vulnerarse la seguridad implementada. Aumentar los tamaños de las claves de cifrado aumenta el tiempo necesario para romperlo, pero no resulta imposible el descifrado. [3]

1.2.3 HERRAMIENTAS AIRCRACK Y COMMVIEW PARA WI-FI

Aircrack es una herramienta para el crackeo de redes Wi-Fi, permite mostrar datos estadísticos y de fuerza bruta sobre los protocolos WEP y WPA. Contiene utilidades principales que son usadas en las fases del ataque y necesario para recuperar la clave. Aircrack-ng puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con COMMVIEW.

1.2.4. ROMPIMIENTO CLAVE WEP UTILIZANDO AIRCRACK

El crackeado de WEP puede ser demostrado con facilidad utilizando herramientas como Aircrack. La meta principal del ataque es generar tráfico para capturar IVs únicos utilizados entre un cliente legítimo y el punto de acceso. Algunos datos

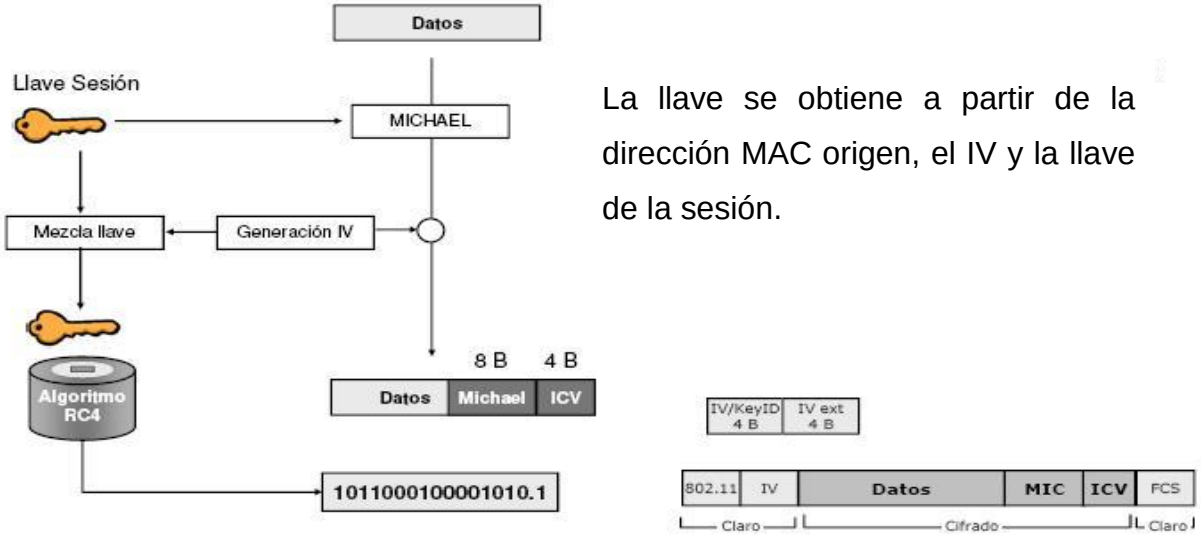
encriptados son fácilmente reconocibles porque tienen una longitud fija, una dirección de destino fija, etc. Esto sucede con los paquetes de petición ARP (*Address Resolution Protocol*), que son enviadas a la dirección broadcast (FF:FF:FF:FF:FF:FF) y tienen una longitud fija de 68 octetos. Las peticiones ARP pueden ser repetidas para generar nuevas respuestas ARP desde un host legítimo, haciendo que los mensajes wireless sean encriptados con nuevos IVs. El primer paso, es la activación del modo monitor en nuestra tarjeta wireless, así que podemos capturar todo el tráfico. El paso siguiente, será descubrir redes cercanas y sus clientes, escaneando los 14 canales que utilizan las redes Wi-Fi. Una vez se haya localizado la red objetivo, se debería a empezar a capturar en el canal correcto para evitar la pérdida de paquetes mientras se escanean otros canales. La inyección empezará cuando una petición ARP capturada, asociada con el BSSID objetivo aparezca en la red inalámbrica. Finalmente, aircrack se utiliza para recuperar la clave WEP. Utilizando el fichero pcap se hace posible lanzar este paso final mientras COMMVIEW sigue capturando datos. [3]

1.3. WPA (*Wi-Fi Protected Access*)

WPA es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Su nombre proviene del acrónimo WPA, es decir, *Wireless Protected Access* (acceso inalámbrico protegido) y tiene su origen en los problemas detectados en el anterior sistema de seguridad creado para las redes inalámbricas. La idea era crear un sistema de seguridad que hiciera de puente entre WEP y el 802.11i (WPA2), el cual estaba por llegar. Para ello utiliza el protocolo TKIP y mecanismos 802.1x. La combinación de estos dos sistemas proporciona una encriptación dinámica y un proceso de autentificación mutuo. Así pues, WPA involucra dos aspectos: un sistema de encriptación mediante TKIP y un proceso de autentificación mediante 802.1x. [4]

1.3.1 FUNCIONAMIENTO DE WPA

Proceso de encriptación



La llave se obtiene a partir de la dirección MAC origen, el IV y la llave de la sesión.

Fig. 3. Proceso de encriptación WPA.

El proceso de encriptación es similar al realizado en WEP, en este caso se utilizan IV de 48 bits, lo que reduce significativamente la reutilización y por tanto la posibilidad de que un hacker recoja suficiente información para romper la encriptación. Por otro lado, WPA automáticamente genera nuevas llaves de encriptación únicas para cada uno de los clientes lo que evita que la misma clave se utilice durante semanas, meses o incluso años.

Por último WPA implementa lo que se conoce como MIC o message integrity code, es decir código de integridad del mensaje. Desafortunadamente es relativamente fácil de modificarlos sin que el receptor lo detecte, a pesar de que los bits de ICV también se encriptan. Para evitarlo se hace uso del MIC (8 bytes, Message Integrity Check), un sistema de comprobación de la integridad de los mensajes, que se instala justo antes del ICV.

Uno de los problemas es el ataque de denegación de servicio (DOS). Si alguien envía dos paquetes consecutivos en el mismo intervalo de tiempo usando una clave incorrecta el punto de acceso elimina todas las conexiones de los usuarios durante un minuto. Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo "Michael" fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo, es aún candidato a ser atacado y debido a ello las redes basadas en WPA implementan un mecanismo de suspensión de 30 segundos en caso de detección de ataque. [4]

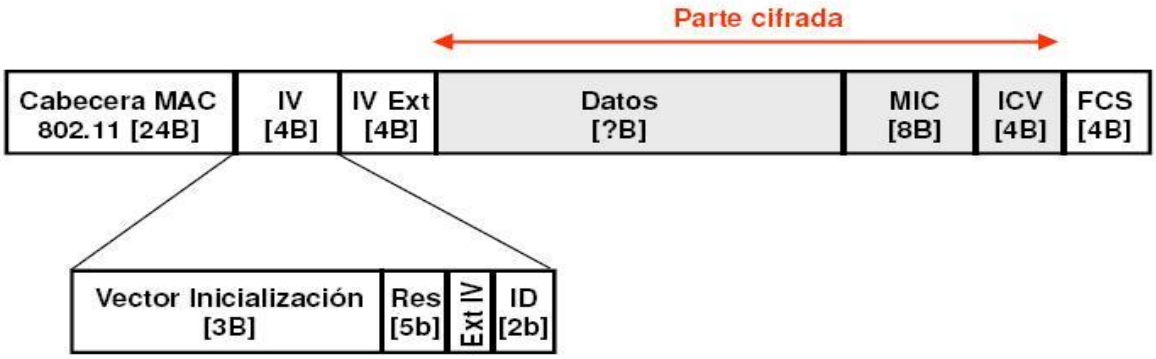


Fig. 4. Trama de datos WPA.

1.3.2. FALLAS DE SEGURIDAD EN WPA

Es vulnerable a ataques de fuerza bruta y por eso incorpora varios contadores para evitar posibles ataques de captura de paquetes o de reinyectado. Pero la debilidad más notoria en este tipo de redes se encuentra en el método de autenticación. Durante este proceso pueden obtenerse los mensajes del resto de conexión o handshake. Otra debilidad, la cual comparte con *WEP*, es el uso de claves compartidas. Como dijimos con *WEP*, el uso de este tipo de claves posibilita que la clave WPA pueda dejar de ser secreta, poniendo en compromiso a todas las estaciones. Aunque se han descubierto algunas pequeñas debilidades en WPA desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. [4]

1.3.3. MEJORAS WPA CON RESPECTO A WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas. Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo. [5]

1.3.4. MODOS DE FUNCIONAMIENTO WPA

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS.
  Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

- Con clave inicial compartida (PSK)
  Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos. [5]

1.3.5. MIGRACIÓN A WPA2

WPA2 es la versión certificada de WPA y es parte del estándar IEEE 802.11i. Hay dos cambios principales en WPA2 con respecto a WPA:

a. El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo “Counter-Mode/CBC-Mac” (CCMP), que es considerado criptográficamente seguro.

b. El reemplazo del algoritmo RC4 por el “Advanced Encryption Standard (AES)” conocido también como Rijndael.

WPA2 fue lanzado en 2004 como un reemplazo para WPA. Este no fue diseñado para ser compatible con WEP en términos de hardware como si lo fue WPA. Además, implementa los elementos obligatorios del estándar IEEE 802.11i-2004. Similar a WPA, WPA2 también utiliza EAP para la autenticación. La característica más importante de WPA2 es la introducción de CCMP que utiliza el Estándar Avanzado de Encriptación (AES). CCMP fue creado para reemplazar TKIP y WEP. CCMP actualmente proporciona el mayor nivel de integridad y confidencialidad disponibles en el estándar 802.11. Todavía no se conocen los ataques posibles contra el algoritmo CCMP, excepto por aquellos ataques de fuerza bruta que intentan descubrir contraseñas débiles. [5]

1.4. TKIP (*Temporal Key Integrity Protocol*)

TKIP fue la primera mejora a nivel de enlace, utiliza el mismo motor de cifrado de flujo RC4 definido para WEP. Sin embargo, TKIP utiliza una llave de 128 bits para el cifrado y las claves de 64 bits para la autenticación. Cada clave es una combinación de una clave de parejas transitoria, la dirección MAC de la estación transmisora, y el paquete de número de serie único de 48 bits. Esta función de mezcla está diseñada para poner la mínima demanda en las estaciones y puntos de acceso, mientras que conserva la fuerza criptográfica suficiente para evitar que se rompan fácilmente.

Una de las bondades de TKIP es que al utilizar el número de serie del paquete como vector de inicialización (IV), también se evita IV duplicados. Además, si se inyectara un paquete con una contraseña temporal que se hubiese podido detectar, el paquete estaría fuera de secuencia y sería descartado.

En cuanto a la llave, esta se genera a partir del identificador de asociación, un valor que crea el punto de acceso cada vez que se asocia una estación. Además del identificador de asociación, para generar la llave se utilizan las direcciones MAC de la estación y del punto de acceso, la clave de sesión y un valor aleatorio. [6]

El protocolo está compuesto de los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.

- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.

- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden. [7]

1.4.1. FUNCIONAMIENTO DE TKIP

La estructura de encriptación TKIP es la siguiente:

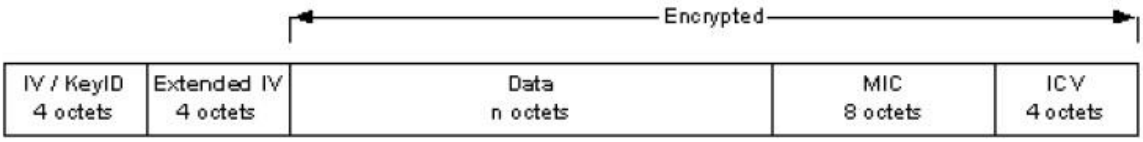


Fig. 5. Proceso de encriptación TKIP.

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de recodificar la llave temporal durante una sola asociación. Pueden intercambiarse 2^{48} paquetes utilizando una sola llave temporal antes de ser rehusada.

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV de 24 bits para su posterior encapsulación WEP. El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

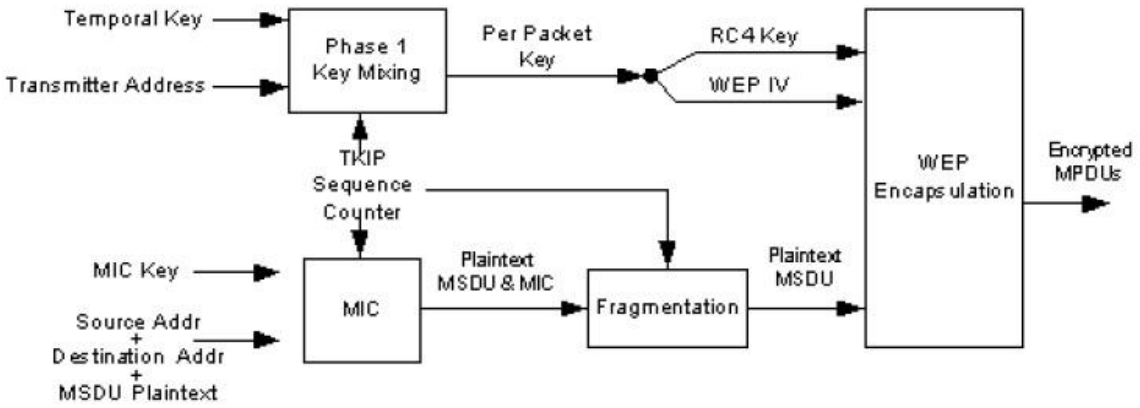


Fig. 6. Proceso de encapsulamiento TKIP.

La función MIC utiliza una función hash unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP. En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Si no, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido. [8]

1.4.2. FALLAS DE SEGURIDAD EN TKIP

TKIP en una versión mejorada de WEP, el cual implementa una mezcla de claves de sesión con un vector de inicialización en cada paquete. Esta mezcla, evita o previene todos ataques a claves actualmente conocidos, puesto que cada byte de cada una de las claves de los paquetes de pende de todos bytes de la clave de sesión y del vector de inicialización (IV). Adicionalmente, un MIC (Message Integrity Check) de 64 bits, más conocido como MICHAEL, es incluido en cada paquete para prevenir ataques al débil mecanismo de protección de la integridad CRC32 conocido desde WEP. Para prevenir ataques de repetición de paquetes, una secuencia de conteo (TSC) es usada, la cual solo permite la llegada de los paquetes en orden al receptor.

TKIP fue diseñado para que fuera compatible con el hardware utilizado por WEP, por lo tanto el algoritmo RC4 y el ICV es todavía incluido en cada paquete.

Ahora bien, es posible desencriptar el tráfico en una red que utiliza TKIP manejando y enviando paquetes con contenido personalizado. Para ello el atacante captura tráfico hasta que encuentra un ARP encriptado, los cuales son fáciles de detectar por las características de su longitud. Adicionalmente, las direcciones IP de la fuente y el destino no son protegidos por WEP y TKIP y las solicitudes son siempre enviadas a direcciones de Broadcast.

La mayor parte del texto plano del paquete es entonces conocido por el atacante, excepto por el último byte de las IPs de origen y destino, el 8 byte del MIC y loas 4 bytes del ICV, de manera que puede ahora llevar a cabo un ataque chopchop para desencriptar los bytes desconocidos en el archivo de texto plano. TKIP implementa principalmente dos contramedidas para evitar estos ataques:

- Si un paquete con un ICV incorrecto es recibido por un cliente, se asume que hay un error en la transmisión y el paquete es descartado. Si este valor es correcto, pero el MIC falla, se asume que hay un ataque y el AP es notificado enviándose un mensaje de error (MIC failure). Si más de 2 fallas de MIC ocurren en menos de 60 segundos la comunicación es terminada y todas las llaves son renegociadas luego de un periodo de penalización de 60 segundos.

- Cuando un paquete ha llegado correctamente, el TSC para el canal por el que se recibió es actualizado. Si un paquete con un valor menor del actual es recibido, es decir que esta fuera de orden, entonces es descartado.

Sin embargo, todavía es posible llevar a cabo un ataque chopchop. El atacante solo necesita elegir un canal de QoS diferente de aquel por donde este fue recibido originalmente. Con un poco más de 12 minutos el atacante puede desencriptar los últimos 12 bytes del texto plano (MIC y ICV), y para determinar los bytes restantes el atacante puede adivinarlos utilizando el ICV desencriptado. Luego de esto, sabiendo el MIC y el texto plano del paquete, ya puede ser revertido el MICHAEL y recuperar la llave MIC utilizada para proteger los paquetes enviados desde el AP al cliente, de manera que el atacante ya es capaz de enviar paquetes personalizados por cada canal QoS, donde el TSC todavía está bajo. Desde este punto ya se puede hacer daño, por ejemplo el atacante, ya conociendo la IP, puede redireccionar tráfico utilizando paquetes ARP falsos. [8]

1.5. CARACTERÍSTICAS DE LOS PROTOCOLOS DE CONTROL DE LA INTEGRIDAD DE LA INFORMACIÓN

Como resultado del análisis de los protocolos de control de integridad de la información descritos en capítulo, a continuación se presenta una tabla comparativa de las características de estos:

	WEP	WPA	WPA2	TKIP
Autenticación	Ninguna	PSK en Modo personal y 802.11x/EAP para empresas.	PSK en Modo personal y 802.11x/EAP para empresas.	PSK en Modo personal y 802.11x/EAP para empresas.
Encriptación	RC4	TKIP/MIC	AES/CCMP	AES
Tamaño de llaves	40 bits para cifrado	128 bits para cifrado	128 bits para cifrado. Llave 256 bits para autenticación en modo personal.	128 bits para cifrado por paquetes y 64 bits para autenticación
Tipo de llaves	Estática. La misma llave se usa en toda la red	Dinámicas. Por usuarios, por sesión, por paquetes.	Dinámicas. Por usuarios, por sesión, por paquetes.	Dinámicas. Por usuarios, por sesión, por paquetes.
Mejoras	N/A	Encriptación mediante TKIP y autenticación mediante el estándar 802.11x.	Reemplazo de MICHAEL por CCMP, y autenticación AES.	Llaves de mayor longitud (128 bits).
Debilidades	Algoritmo de encriptación débil RC4. Ivs cortos (24 bits). Débil detección de errores (CRC32).	Mensajes de handshake vulnerables durante la autenticación.	Se puede lanzar un ataque de denegación de servicio debido 4-way handshake durante la autenticación.	Ataque de redireccionamiento de tráfico debido a los ARP request visibles en la red. Ataques chopchop a los textos planos.

CAPÍTULO 2

SIMULADORES DE RED

2.1 **INTRODUCCIÓN**

En este capítulo se intenta tener un primer acercamiento a aquellas herramientas que permitirán con respecto a los simuladores pertinentes para la defini, las cuales son los simuladores de red. Se describirán las características de algunos simuladores con el fin de seleccionar el que más se adapte a nuestra necesidad y de esta manera realizar la tarea de definir la arquitectura de red en un escenario VANET.

Algunos de estos simuladores consisten solo en un conjunto de clases y funciones de programación por lo que será complejo describirlos. De la misma manera, se necesitarán conocimientos de los protocolos de red a simular para poder tener argumentos y explorar de manera más eficaz las bondades de estos, por lo cual es útil la información descrita en el capítulo.

2.2 **DEFINICIÓN DE SIMULACIONES**

Definimos simulación como una técnica que imita el comportamiento de un sistema del mundo real conforme evoluciona en el tiempo. Por lo tanto, se podrá analizar y observar características, sin la necesidad de acudir al sistema real.

Surgen pues, de éste concepto, dos nuevas definiciones:

- Modelo de simulación que se refiere al conjunto de hipótesis acerca del funcionamiento del sistema expresado como relaciones matemáticas y/o lógicas entre los elementos del sistema.
- Proceso de simulación que será la ejecución del modelo a través del tiempo en un ordenador para generar nuestras representaciones del comportamiento del sistema.

En resumen, podemos decir que el modelo hace referencia a la representación del sistema real que vamos a analizar, las condiciones de su funcionamiento, y las

variables que emplea. En cambio, el proceso hace referencia a una ejecución concreta, con unos valores asociados a las variables que se pueden ajustar en el modelo, y que se realiza para obtener los resultados referidos a ciertos parámetros que especifican el comportamiento del sistema. [9]

La simulación se limita a informar de cuál sería el comportamiento del sistema analizado en las condiciones que se indiquen para un proceso determinado.

Otro punto a tener en cuenta son los resultados obtenidos por el simulador. El proceso se basa en el muestreo aleatorio, es decir, los resultados que de él se extraigan, están sujetos a variaciones aleatorias y por este motivo los resultados obtenidos han de ser examinados. Por lo tanto, los resultados tendrán que ser evaluados y comprobar si éstos resultados son fiables o no conforme a las previsiones que se tenían antes de realizar dicho proceso.

Otra definición muy importante corresponde a la de sistema. Un sistema es un conjunto de elementos que actúan e interactúan para lograr algún fin lógico. Cuando hablamos de estado del sistema hacemos referencia al conjunto de variables necesarias para describir el estado del sistema en un determinado instante de tiempo. Entre todas estas variables tenemos que distinguir las entradas y las salidas. Las salidas serán los objetivos de nuestro estudio, expresados mediante valores numéricos. [10]

Las entradas serán los valores numéricos que permitan iniciar la simulación y obtener las salidas. En estas entradas, se incluyen:

- Las condiciones iniciales: Valores que expresan el estado del sistema al principio de la simulación.
- Datos determinísticos: Valores conocidos necesarios para realizar los cálculos que producen las salidas.
- Datos probabilísticos: Cantidades cuyos valores son inciertos pero necesarios para obtener las salidas del sistema. Los valores específicos de estos datos deben conocerse a través de una distribución de probabilidad.

2.3 **NECESIDAD DE LOS SIMULADORES**

Es claro que existe un crecimiento vertiginoso en el desarrollo de las tecnologías de comunicación, así como la implementación de estas por parte de los actores

de la industria. Es imprescindible entonces pensar en la utilización de herramientas que permitan en definitiva, abaratar los costos de diseño y mejorar la calidad y reducir el tiempo de lanzamiento de un producto al mercado “time-to-market”.

Entre estas herramientas encontramos los simuladores, que juegan un papel fundamental puesto que permiten realizar pruebas a distintos niveles, en modelos simplificados de la realidad y que posibilitan aumentar la flexibilidad de los resultados.

2.4 **VENTAJAS SIMULADORES**

- *Aumentar la productividad en el desarrollo de redes.*
  Acelerar los tiempos de desarrollo en una ventaja clave que proporcionan las herramientas de simulación, gracias a que estas se configuran como un instrumento que permite obtener resultados cercanos a la realidad, y que posteriormente pueden ser analizados para la toma acertada de decisiones.

- *Mejorar la calidad del producto.*
  Ciertamente el simulador permite probar el producto o servicio en escenarios realistas mucho antes de que este sea lanzado al mercado.

- *Reducir el Time-to-Market.*
  La validación de los diseños hecha gracias a las herramientas de simulación se convierte en una ventaja en el momento en que el tiempo de desarrollo del producto o servicio se disminuya permitiendo que puedan salir al mercado mucho antes que la competencia.

- *Permitir estudiar sistemas complejos.*
  Los simuladores permiten estudiar sistemas en los cuales no es posible obtener resultados analíticos, o bien estos resultados son solo una referencia obtenida de las simplificaciones efectuadas.

2.5 ALCANCE DE LOS SIMULADORES

Las diversas características de los simuladores llegan a brindarnos los siguientes beneficios:

- Permiten simplificar el proceso de desarrollo gracias herramientas gráficas, protocolos predefinidos, herramientas de análisis y depuradores.
- Permiten un modelado conforme a los parámetros a medir.
- Son escalables y configurables.
- Permiten diferenciar cuáles son las simplificaciones del modelo y su alcance.
- Brindan la posibilidad de definir distintos escenarios.
- Algunos tienen una arquitectura abierta que permite el desarrollo de protocolos propios o especificaciones particulares.
- Brindad rendimiento gracias a las velocidades de simulación.

2.6 SITUACIÓN ACTUAL DE LOS SIMULADORES

Los simuladores de redes son herramientas ampliamente usadas en el mundo de la ingeniería. Permiten modelar redes de computadores completas definiendo los comportamientos específicos de sus nodos, dispositivos y enlaces en un escenario virtual con el que se puede interactuar. Es por esto que se convierten en una herramienta relativamente barata y rápida en comparación con lo que supone el montaje de una red real para experimentación. Los simuladores son también especialmente útiles para los diseñadores, ya que les permiten probar nuevos protocolos o cambios en protocolos existentes en un entorno controlado.

Los simuladores de redes suelen disponer de una amplia variedad de tecnologías de red y de herramientas para ayudar al usuario a construir redes jerárquicas complejas a partir de bloques básicos (pueden ser nodos, enlaces, perfiles de tráfico, eventos meteorológicos, etc.).

La mayoría de herramientas de simulación de redes se basan en el paradigma de la simulación de eventos discretos (discrete event-based simulation). Esto implica que los nodos de la red lanzan eventos para indicar su actuación, por ejemplo cuando envían un paquete a otro nodo, mientras que el simulador a su vez

mantiene una lista de eventos ordenada según el tiempo de ejecución. La simulación se termina correctamente cuando se procesan todos los eventos que se encuentren en cola.

Uno de los simuladores más potentes y flexibles de los utilizados en el entorno empresarial es OPNET Modeler. Esta herramienta es paga, pero también se distribuye gratuitamente a universidades para su uso con fines docentes y de investigación. Esta opción, es la que ha permitido usar este simulador en el desarrollo de esta monografía. [11]

2.7 **TIPOS SIMULADORES**

Existen diversos tipos de simuladores, distinguidos según los parámetros que deseemos modelar y analizar. A veces nos es fácil establecer la separación entre ellos, de hecho normalmente existen combinaciones de estos tipos.

- Simulador de Red (System Level): analizar tráfico generado en la red, QoS handovers, control de admisión, gestión de carga… Utilizan resultados del simulador de nivel de enlace.
- Simulador nivel de Enlace (Link level): protocolos nivel enlace, control de errores. Por ejemplo, muy usados en UMTS para evaluar el rendimiento del uso de W-CDMA o TD-CDMA en a interfaz radio UTRA. Utilizan resultados del simulador de capa física o lo incluyen.
- Simulador capa física: cobertura, potencia, células, análisis de obstáculos.
- Simulador protocolos: verificar, analizar y optimizar protocolos.

2.8 **DESCRIPCIÓN DE LOS SIMULADORES**

2.8.1 OMNeT++

Omnet es una herramienta de modelado y simulación pública, basado en componentes modulares, con un ambiente de simulación de arquitectura abierta y con un fuerte soporte de GUI., creado por András Varga en el 2003 en la Universidad Técnica de Budapest. Es un simulador de ambiente discreto. Su área de aplicación primaria es la simulación de redes de comunicación, y debido a su arquitectura genérica y flexible, ha sido utilizada exitosamente en redes basadas

en colas de espera y arquitectura de hardware. Múltiples modelos de simulación de fuente abierta han sido publicados, en el campo de las simulaciones de Internet (IP, IPv6, MPLS, etc.), movilidad, simulaciones ad-hoc y otras áreas.

Gracias a la arquitectura modular que provee Omnet, cuyos componentes (módulos) están programados en C++, éstos módulos después puedes ser ensamblados en componentes y modelos más grandes utilizando un lenguaje de alto nivel (NED). Su soporte de GUI, junto con su arquitectura modular permite que las simulaciones puedan ser incluidas fácilmente en aplicaciones propias.

Omnet proporciona las herramientas básicas para realizar simulaciones, pero por sí mismo no proporciona ningún componente específico para la simulación de redes de computadoras, simulaciones de colas, simulaciones de arquitectura de sistemas o cualquier otra área. En su lugar, estas áreas de aplicación son proporcionadas por varios modelos de simulación y arquitecturas tales como Mobility Framework o INET Framework. Estos modelos son desarrollados completamente independientes a lo que es Omnet, y siguen sus propios ciclos.

Así pues, lo que Omnet proporciona en sí es una librería clase C++ que permite la creación de componentes de simulación como módulos simples y canales; también, se proporciona la infraestructura para reunir las simulaciones de estos componentes y configurarlos en el lenguaje NED o en archivos tipo *ini*. Proporciona además interfaces donde se puede observar y manipular el tiempo de ejecución o ambientes para la simulación como *Tkenv, Cmdenv*; herramientas para facilitar crear simulaciones y evaluar sus resultados como *GNED, Scalars y Plove*. [12]

Para poder realizar una simulación en Omnet se pueden seguir unos pasos básicos, que en general, pueden ser aplicados para el modelado. A continuación un vistazo rápido de cómo utilizar Omnet:

a. Un modelo Omnet se construye a partir de componentes (módulos) que se comunican mediante el intercambio de mensajes. Los módulos pueden estar anidados, es decir, varios módulos se pueden agrupar para formar un módulo compuesto. Al crear el modelo, es necesario asignarle al sistema una jerarquía de módulos de comunicación.

b. Definir el modelo de estructura en el lenguaje NED. Puede editar la NED en un editor de texto o en el editor gráfico del Omnet basado en Eclipse + +.

c. Los componentes activos del modelo (módulos simples) deben ser programados en C++, utilizando el núcleo de simulación y la biblioteca de clases.

d. Proporcionar un omnetpp.ini propicio para la configuración y los parámetros de su modelo. Un archivo de configuración se puede describir varios procesos de simulación con parámetros diferentes.

e. Crear el programa de simulación y de ejecución. Se vincula el código con el núcleo de simulación del Omnet y una de las interfaces de usuario proporcionadas por Omnet. Hay línea de comandos e interfaces gráficas de usuario interactivas. [13]

2.8.2 QualNet

QualNet es un simulador para redes heterogéneas a gran escala, así como simula las aplicaciones distribuidas que se ejecutan en estas redes.

Las siguientes características de QualNet proporcionar una capacidad única para la simulación precisa y eficiente de redes heterogéneas a gran escala:

- Robusto conjunto de protocolos de red cableada e inalámbrica y los modelos de equipos, útiles para la simulación de diversos tipos de redes.
- Optimizada para la velocidad y escalabilidad en un procesador, QualNet ejecuta escenarios equivalente a 5-10x veces más rápido que las alternativas comerciales.
- Diseñado desde cero como un simulador paralelo, QualNet ejecuta la simulación mucho más rápido a medida que agrega más procesadores.
- Una interfaz gráfica de usuario robusto cubre todos los aspectos de la simulación, desde la creación de escenarios y la configuración de la topología, la integración de los protocolos personalizados, a través de la ejecución en tiempo real de los modelos de red desde dentro del GUI, animaciones, hasta análisis estadístico de la simulación.

- QualNet se ha utilizado para simular los modelos de alta fidelidad de las redes inalámbricas con hasta 50.000 nodos móviles. [14]

QualNet ofrece una gama de herramientas que interactúan entre sí, de forma que consiguen dar solución a redes complejas, mediante una interfaz de alto nivel. Los elementos que forman parte de esta familia de aplicaciones son:

- QualNet Library: Es una colección de modelos de red en fuente para facilitar el desarrollo del sistema modelo y del código del sistema completo.
- QualNet Simulation Engine: El motor de simulación es escalable, adaptado a modelos de alta exactitud para redes con alto número de nodos. El buen empleo de los recursos de cálculo consigue que el modelado de redes de gran escala con tráfico pesado y teniendo en cuenta factores de movilidad, consigue resultados en tiempos razonablemente cortos.
- QualNet Graphical User Interface: Interfaz gráfica de usuario.
- Scenario Designer: Es una herramienta para la configuración del experimento de manera gráfica- Define la distribución geográfica, conexiones físicas y parámetros de funcionamiento de los nodos de la red.
- Animator: Es utilizado para visualizar la simulación mientras se está ejecutando.
- Protocol Designer: Es una máquina de estados finitos, para el modelado de protocolos, mediante una interfaz gráfica intuitiva.
- Analyzer: Es la herramienta de representación de los datos estadísticos procedentes de las simulaciones.
- Packet Tracer: Es una aplicación de nivel de paquetes para visualizar el contenido de los paquetes mientras ascienden o descienden de la torre de protocolos.[15]

2.8.3 OPNET Modeler

OPNET Modeler es un software comercial que proporciona un entorno de desarrollo para el modelado y la simulación de redes, componentes, protocolos y aplicaciones de forma flexible y escalable. Utiliza un modelado orientado a objetos y un entorno gráfico para componer intuitivamente las redes haciendo uso de módulos que representan componentes actuales de las redes de telecomunicaciones.

Existen gran variedad de módulos que podemos añadir al programa, para construir el entorno que se quiera someter a estudio. En nuestro caso, son de especial interés los módulos Wireless que permitan evaluar el desempeño de las redes inalámbricas en escenarios móviles. Este módulo de ampliación proporciona a OPNET una amplia gama de protocolos desarrollados como MAC, protocolos de alto nivel y aplicaciones.

Así mismo, incluye el modelado de efectos de transmisiones en redes Wireless como:

- Propagación RF (pérdidas por difracción, efectos atmosféricos, vegetación…)
- Interferencias.
- Características de los transmisores y receptores
- Nodo en movimiento.

Otras de las características más importantes son:

- Se pueden realizar modelados de máquina de estados finitos para el diseño de protocolos y de otros procesos.
- Wireless, punto-a-punto y enlaces multipunto de forma abierta y programable. Se pueden definir con exactitud los parámetros de retrasos, disponibilidad, errores de bit y tasas de salida en cada enlace. Se incluyen características de capa física y efectos de entorno.
- Capacidad para realizar modelado geográfico y de movilidad.
- APIs para la programación asistida o inspección de los modelos y de los archivos de resultados. Se pueden integrar fácilmente las librerías de código existentes en las simulaciones. Se provee el código de todos los modelos estándares.
- Herramientas de análisis integradas
- Podemos animar el comportamiento del modelo durante o al finalizar la simulación.
- Depurador Integrado.
- Librería detallada de modelos de protocolos y aplicación (Voz, HTTP, TCP, IP, OSPF, BGP, EIGRP, RIP, RSVP, Frame Relay, FDDI, Ethernet, ATM, 802.11 Wireless LANs, MPLS, PNNI, DOCSIS, UMTS, IP Multicast, Conmutación de paquetes,…)

OPNET tiene por contra, que es software propietario, con un precio de licencia muy elevado. Sin embargo existe una solución que no es propietario y es la versión OPNET IT Guru Academic Edition.

2.8.4 OPNET IT Guru Academic Edition

OPNET IT Gurú proporciona un entorno virtual de red que modela el comportamiento de una red por completo, incluyendo sus pasarelas (routers), conmutadores (switches), protocolos, servidores y aplicaciones en red. Este entorno de trabajo es de gran utilidad para los responsables de informática e I+D, diseñadores de redes, operadores y personal de mantenimiento de red, etc. ya que permite diagnosticar problemas de una forma eficiente, validar cambios en la red antes de implementarlos y prever el comportamiento de la red ante futuros escenarios como crecimiento de tráfico, fallos de red, etc. [16]

Limitaciones

La versión académica del OPNET It Guru tiene algunas limitaciones como las son las siguientes:

- Limitaciones de Importación: los escenarios creados en cualquiera de las otras versiones comerciales de OPNET no pueden ser importados hacia esta version académica. Solo pueden ser importados escenarios creados con esta misma versión.
- Limitaciones de exportación: de la misma manera como sucede con las importraciones, los escenarios creados con la version académica no pueden ser exportados hacia las otras versiones comerciales.
- Limitaciones de modelado: esta version no incluye algunos módulos como Flow Analysis, Net Doctor, Terrain Modeling, etc. Esta versión no es la MODELER, asi que los modelos no pueden ser modificados. Tampoco es posible importar un modelo creado con el OPNET Modeler.
- Limitaciones de las Características Inalámbricas: Los estados “Pipe-Line”, usados en el modelo inalámbrico, no pueden ser modificdos como en el Modeler. En este sentido, todas las transmisiones utilizarían el modelo de “space loss attenuation”. Tampoco se tiene el editor de antenas, y además todas los nodos inalámbricos usarían el modelo de antena isotropica.
- Se pueden crear nodos móviles, pero no nodos satelitales como en el Modeler.

- Los proyectos creados en esta edición son limitados en el número de dispositivos multipuertos. Se pueden correr pequeñas simulaciones con un número razonable de elementos de ruteo (20) para propositos educativos pero no comerciales. [17]

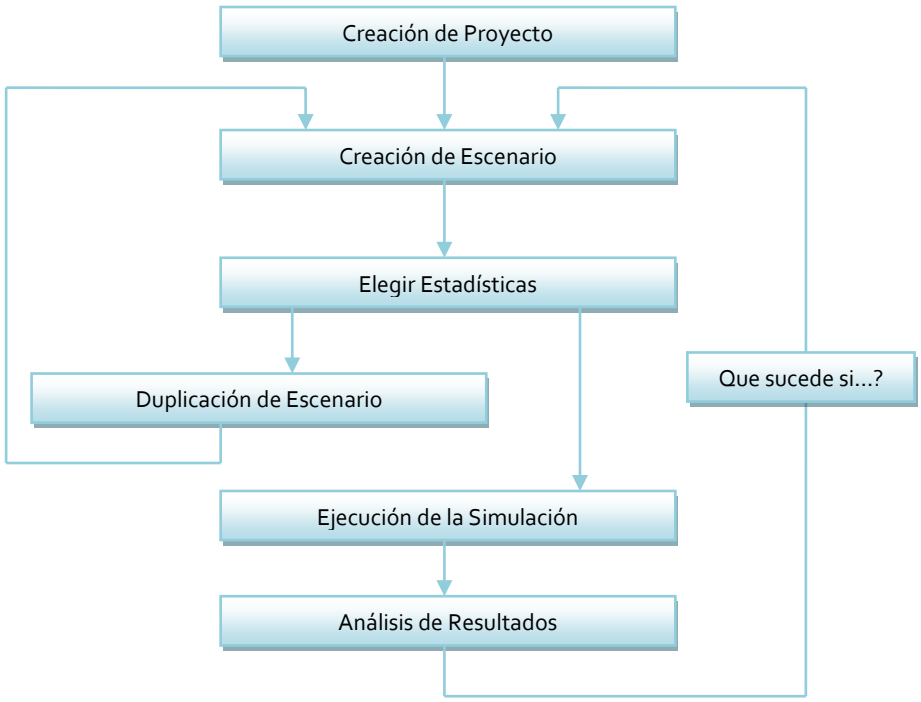


Fig 7.Diagrama del uso del Simulador

2.8.5 Network Simulator 2

Ns2 es un simulador de eventos centrado en la investigación sobre redes. Dispone de simulación para TCP, routing y multicast sobre redes cableadas o inalámbricas (locales y por satélite).

Ns empieza como una variante del REAL NETWORK SIMULATOR en 1989 y ha evolucionado substancialmente durante los últimos años. En 1995 el desarrollo lo llevaba a cabo DARPA, Xerox PARC, UCB y USC/ISI. Actualmente el desarrollo de ns lo lleva DARPA junto a SAMAN y otros. Ns siempre ha contado con

contribuciones de muchos otros desarrolladores, incluyendo código inalámbrico de los proyectos CMU Monach y UCB Daedelus y también de Sun Microsystems. [9]

Actualmente NS-2 sigue desarrollándose a través de CONSER (Collaborative Simulation For Education and Reserch) que tiene como objetivo:

- La investigación en el desarrollo y evaluación del protocolo de red.
- Enseñanza de los protocolos de red nuevos como existentes.

Y SAMAN (Simulation Augmented by Measurement and Analysis for Networks), el cual se dedica a extender, detectar, y predecir fallos en el simulador. Además de los mencionados hay otros colaboradores como ACIRI.

El simulador consta de un núcleo principal escrito en C++ que se puede ejecutar simplemente tecleando *ns* en la línea de comandos. Para actuar sobre el simulador se utiliza una interfaz específica. Este interfaz es oTcl que deriva del Tcl pero orientado a objetos. [18]

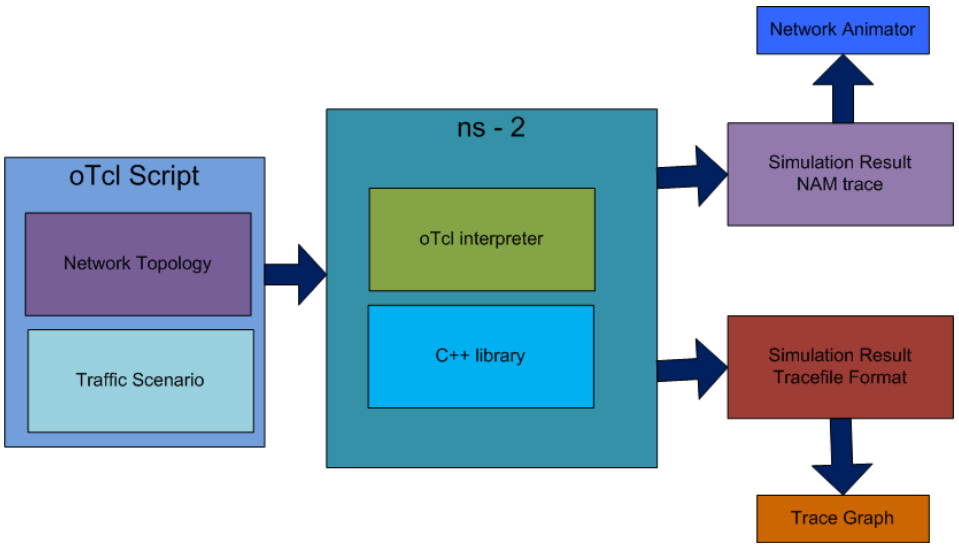


Fig. 8. Funcionamiento NS-2.

¿Qué se puede hacer con NS-2?

a. Podemos definir:

- Redes terrestres, inalámbricas y por satélite con varios algoritmos de enrutado (DV, LS, PIM-DM, PIM-SM, AODV, DSR).
- Distintas fuentes de tráfico: Web, ftp, telnet, cbr, etc...
- Fallos como perdidas probabilísticas y deterministas, fallos en la conexión, etc.
- Distintas disciplinas de encolado (drop-tail, RED, FQ, SFQ, DRR, etc.) y QoS (calidad de servicio, como por ejemplo IntServ y Diffserv).

b. Podemos visualizar:

- Flujo del paquete, su encolado y su posible descarte.
- Comportamientos del protocolo: comienzo lento de TCP, control de congestión, retransmisión rápida y recuperación.
- Movimiento de nodos en redes inalámbricas.
- Notas de los sucesos más importantes.
- Estados del protocolo.

2.8.6 Network Simulator 3

Ns-3 es un nuevo simulador de red de eventos discretos que pretende convertirse en el sucesor de ns-2. El proyecto está financiado por la NSF-CISE (National Science Foundation, Computer & Information Science & Engineering). Ns-3 tiene su punto de partida en el trabajo de Mathieu Lacage en el simulador yans (Yet Another Network Simulator), durante el cual se identificaron en Ns-2 un conjunto de fallos de diseño que juzgaron lo suficientemente como para iniciar un nuevo simulador desde cero. Entre estos fallos destacaban la falta de versatilidad, debido básicamente a la dependencia entre los modelos (acoplamiento), el deficiente uso de las técnicas de programación orientada a objetos, y el rígido acoplamiento entre C++ y OTcl.

A diferencia de su predecesor, ns-3 está desarrollado exclusivamente en C++, aunque permite el interfaz con lenguajes de alto nivel (por ahora sólo Python). Los

antiguos scripts para ns-2 (desarrollados en OTcl) no funcionan en ns-3. Ns-3 es un proyecto reciente (iniciado en junio de 2006) y está planificado que el desarrollo de su código base se extienda hasta 2010.

Características de NS-3:

a. Protocolos inalámbricos que soporta:

- 802.11a: El desarrollo original implementa completamente 802.11a en modo infraestructura (AP/cliente) y ad-hoc (el código lo hereda de yans).
- 802.11b: Guangyu Pei y Tom Henderson presentaron en el Wns3-2009 (2009 Workshop on ns-3) una propuesta para el desarrollo del modelo y su validación, pero no hay todavía código disponible de su implementación.
- 802.11e: De los dos tipos de acceso que contempla HCF (Hybrid Coordination Function), ns-3 implementa EDCA (Enhanced Distributed Channel Access) y está en desarrollo el soporte para HCCA (Controlled Access).
- 802.11g: No se ha encontrado ninguna referencia a la implementación del modo g.
- 802.16-2004: Existe una implementación de 802.16-2004 (anuncio, documentación, código), pero sólo implementa el modo PMP. Consultado el mantenedor actual del paquete, en estos momentos no está previsto extender el soporte a redes Mesh.

b. Nodos multi-interfaz: La herramienta es muy versátil, es posible añadir tantos interfaces como se desee, de la tecnología que sea, en cada nodo.

c. Encaminamiento: Si la simulación no está orientada a pruebas específicas de encaminamiento, por simplicidad se emplean una tabla de enrutado centralizada y única (objeto GlobalRouteManager). Además, existen implementaciones para encaminamiento estático (tanto para unicast como multicast) y OLSR (Optimized Link State Routing). La implementación de Quagga está en desarrollo. Nivel físico configurable.

d. Pérdida de paquetes: Soportada, a partir del cálculo del SNR y la BER (en función de la modulación empleada).

e. SNR/BER externo: Como en el resto de simuladores no existe esta opción, se tendría que implementar.

f. Simulaciones distribuidas: No soportado en este momento, aunque es uno de los objetivos del simulador desde el inicio y está prevista como tarea para el GSC-2009 (Google Summer of Code).

g. Simulación de aplicaciones/protocolos reales: No soportado, aunque se está trabajando para ofrecer una API similar a la de los sockets BSD para facilitar el desarrollo de aplicaciones para ns-3. Por otra parte, está en desarrollo portar NSC a ns-3, lo que permitiría usar implementaciones reales del protocolo TCP (con el objetivo de, al menos, poder simular con elkernel de Linux).

h. Modo de emulación: Soportado, una simulación ns-3 puede enviar datos a través de redes reales a otros nodos de simulación ns-3.

i. Modo de comandos/GUI: Por el momento todas las operaciones se hacen por línea de comandos. No hay herramientas gráficas, aunque están en desarrollo aplicaciones que permitirán visualizar simulaciones a través de un GUI. [19]

2.9. EVALUACIÓN DE LOS SIMULADORES

2.9.1. TABLA DE PONDERACIÓN

Simulador	Orientación y Área de Uso / 20pts	Requerimientos del Sistema y del S.O. / 10 pts	Características generales / 20pts	Protocolos y Tecnologías / 20 pts + 10 pts por soporte de framework	Tipo de Licencia / 10pts
Caracteristicas	Orientado a seguridad en redes inalámbricas con arquitectura móvil	Soporte multiples sistemas operativos	Arquitectura modular, orientación a objetos, presentación de resultados.	Protocolos de routing, transporte, redes móviles (AODV, DSVD, DSR, TDMA, CDMA, etc.). 10 puntos adicionales si soporta framework con arquitectura VANET.	tipo de licencia gratuita o abierta para usos académicos

2.9.2. Tabla Comparativa de Simuladores

Simulador	Orientación y Área de Uso	Requerimientos del Sistema y del SO.	Características generales	Protocolos y Tecnologías	Tipo de Licencia
Omnet++	Simulador de redes cableadas e inalámbricas, redes on-chip, redes de cola. Soporta simulaciones de redes de sensores, redes ad-hoc, redes fotónicas entre otras.	Linux x86 (32-bit / 64-bit), Windows 7, Vista, XP (32-bit), Mac OS X 10.5 and 10.6 (32-bit). Necesita Java runtime (JRE)	Arquitectura modular. Módulos programados en C++. Proporciona interfaces para manipular ambientes de simulación y evaluación de resultados.	Librerías de simulación implementadas en c++. Compilador para el lenguaje editor de redes NED. GUI llamada tkenv. Graficación de Vectores y escalares mediante Plove y Scalars. Se puede integrar frameworks especializados para un mejor modelamineto. Uno de ellos en el INETMANET.	Gratis para usos académicos y sin ánimo de lucro. Licencias para fines comerciales en omnest.com
Network Simulator 2	Permite definir redes terrestres, inalámbricas y por satélite con varios algoritmos de enrutado (DV, LS, PIM-DM, PIM-SM, AODV, DSR).	Trabajo sobre plataformas UNIX/linux y Cygwin para windows 9x/2000/xp.	Soporte de arquitectura orientada a objetos. Librerías en C++. Panificador de eventos discretos. Script que describen la arquitectura de la simulación y los escenarios (TCL)	Protocolos de red cableadas: Unicast, Multicast, and Hierarchical Routing, TCP, UDP, web, ftp, telnet, cbr, drop-tail, RED, IntServ and Diffserv Wireless Networking. Redes Móviles: AODV, DSDV, DSR, TDMA, CDMA, IEEE Mac 802.x.	GNU General Public License (GPL) version 2 (software libre).

Simulador	Orientación y Área de Uso	Requerimientos del Sistema y del S.O.	Características generales	Protocolos y Tecnologías	Tipo de Licencia
Qualnet	Simulación de redes cableadas e inalámbricas y medición de desempeño de dispositivos de redes. Diseñado para obtener la mayor ventaja de multihilos de procesadores de arquitectura multinucleo	Linux. Windows. Mac OS X. Procesador 32-64 bits (x86 , x64 compatible). Memoria 128MB - 4GB dependiendo del número de nodos. 600MB disco duro.	QualNet ofrece portabilidad de su plataforma y flexibilidad de la interfaz. Se ejecuta en paralelo y secuencial con Unix, Windows, Mac OS X y Linux, también está diseñado para conectar con aplicaciones modelado/simulación y redes en vivo.	Las librerias soportan: WANs, LANs, IPv6, abstract satellite, 802.11a/b/g, mobile ad-hoc networks, WiMAX, VoIP, queueing,scheduling, MPLS, y otras QoS, GSM, modelado de redes con, encriptación, autenticación, llaves de seguridad, certificados, IEEE 802.15.4 (ZigBee) andsensor networks	Esta herramientaes de tipo propietario.
Opnet Modeler	Simulación y modelamiento de todo tipo de redes y tecnologías incluyendo: VoIP, TCP, OSPFv3, MPLS, IPv6	Procesador 500 Mhz o más.256 MB de memoria RAM, 400 MB de espacio en disco, Pantalla: 1024 x 768 o mayor resolución, 256 colores o más, Windows NT/2k/XP	Modelado de alta fidelidad diseñado bajo el esquema de editores jerárquicos para la estructuración de redes reales, equipos y protocolos. Estos son el editor de proyectos, el de nodos y el de procesos.	BGP, HAIPE, IPv6, LTE, MANET (AODV, DSR, GRP, OLSR, OSPFv3, TORA), MPLS, RIPng, Satellite technology, SIP, TCP, TDMA, UMTS, VLAN, VoIP, VPN, WiMAX (802.16e), WLAN (802.11a, b, e, g), ZigBee (802.15.4).	Esta herramientaes de tipo propietario.

Simulador	Orientación y Área de Uso	Requerimientos del Sistema y del S.O.	Características generales	Protocolos y Tecnologías	Tipo de Licencia
Opnet It Guru	Orientado a la simulación de algunos tipos de redes y protocolos, no permite modelado puesto que es una herramienta dirigida a la comunidad académica.	Windows NT 4.0/2000/XP/Vista/7. Procesador 500Mhz. RAM: 256MB. Espacio en Disco: 200MB. Resolución: 1024x768 o superior 256 colores o más.	Proporciona un entorno virtual de red que modela el comportamiento de una red por completo. Permite diagnosticar problemas de una forma eficiente.	HTTP, TCP, IP, OSPF, BGP, EIGRP, RIP, RSVP, Frame Relay, FDDI, Ethernet, ATM, 802.11 Wireless LANs, MPLS, PNNI, DOCSIS, UMTS, IP Multicast.	Se distribuye gratuitamente a universidades para su uso con fines docentes y de investigación.
Network Simulator 3	Su objetivo desarrollar un entorno preferido para la simulación de redes abiertas de investigación. Alentar hacia la contribución de la comunidad, la revisión y validación del software.	Sistemas POSIX como GNU/Linux, BSD, OS X y Microsoft Windows (con Cygwin o MinGW). Procesador 500Mhz. RAM: 256MB. Espacio en Disco: 180MB.	Permite la utilización de dos lenguajes de programación, C++ y Python, para la descripción de modelos y lógica de simulación. Permite características de bajo nivel de la API, ofreciendo flexibilidad al permitir al usuario configurarla de diferentes maneras.	Permite redes IP y no IP. Especializado para la simulación de redes wireless/IP que involucra modelos Wi-Fi, WIMAX o LTE y variedad de protocolos dinámico o estáticos como OLSR y AODV.	Licencia de gratuita de código abierto. GNU GPL v2.

2.9.3. SELECCIÓN DE SIMULADOR

Simulador	Orientación y Área de Uso / 20pts	Requerimientos del Sistema y del S.O. / 10 pts	Características generales / 20pts	Protocolos y Tecnologías / 20 pts + 10 pts por soporte de framework	Tipo de Licencia / 10pts	TOTAL
OMNET++	20	20	20	20	20	100
NS2	20	20	15	0	20	75
QUALNET	20	20	20	0	0	60
OPNET MODELER	20	20	20	0	0	60
OPNET IT GURU	0	20	20	0	20	60
NS3	20	20	20	0	20	80

La anterior tabla muestra los puntajes obtenidos por cada simulador referentes a los parametros descritos en el numeral 2.9.1.

El simulador seleccionado fue OMNET++ al sumar 100 puntos debido a que esta orientado a usos académico en redes inalámbricas, Sus especificaciones minimas de sistema operativo y hardware concuerdan con los requerimientos de arquitectura de red necesarios para la ilustracion de un escenario de redes VANETS. Además dentro de las características generales permite arquitectura modular, asi mismo y más importante permite el uso de frameworks y existe en este caso uno muy pertinente el cual es INETMANET. Finalmente no es herramienta de uso propietario, por el contrario es de uso gratuito para fines académicos.

CAPÍTULO 3

ARQUITECTURA DE VANETS EN OMNET++ Y CRACKEO DE WEP Y WPA

3.1. INTRODUCCIÓN

Con el fin de mostrar el comportamiento de los elementos de una red VANET, en este capítulo se definirán las características de la arquitectura de una red de este tipo para el simulador OMNet++, a través de la implementación de un framework que predefine topologías y arquitecturas de redes y nodos ad-hoc.

Adicional, se describirán los pasos a seguir para configurar el OMNeT++ y el framework INETMANET que posibilita la emulación de nodos móviles en una red VANET. Además se hará uso del software COMMVIEW y AIRCRACK para realizar un ejercicio de crackeo del protocolo WEP a fin de mostrar su vulnerabilidad.

Finalmente se muestra un comparativo de los protocolos resaltando las características de estos.

3.2. ARQUITECTURA DE LA SIMULACIÓN

Para la configuración de un entorno móvil se utilizan tres módulos principales dentro del espacio de trabajo, que hacen referencia a los componentes que interactuarán entre sí para llevar a cabo la simulación.

Estos tres módulos son:

a. Channelcontrol, el cual define las características del canal. Estas son el tamaño del espacio físico donde se simula, la máxima potencia de la señal de las NICS para esta red (mW), el parámetro de atenuación de la señal (dBm), el coeficiente de la perdida de ruta de los nodos, la frecuencia del canal y el número de canales.

b. Flat Network Configurator, el cual define parámetros tales como direcciones de red y mascara de red, que se encuentran predeterminadas en esta simulación a 192.168.0.0 y 255.255.0.0 respectivamente.

c. Host, el cual modela un nodo móvil con una tarjeta de red inalámbrica (802.11b) en modo ad-hoc. Este modelo contiene la implementación IEEE 802.11 y los protocolos IP, TCP y UDP.

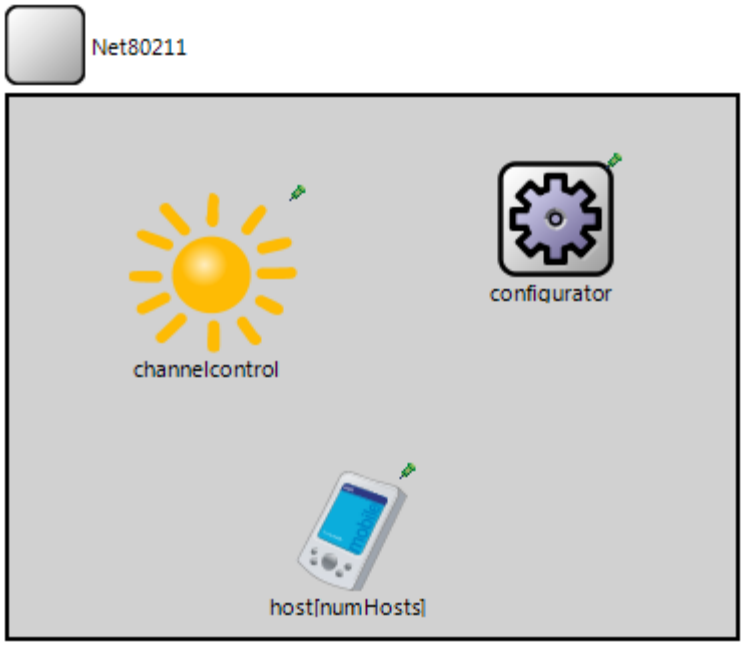


Fig. 9. Arquitectura de simulación OMNeT++

3.3. ARQUITECTURA DE NODOS

Los nodos hosts implementados en esta red están compuestos por los siguientes módulos:

a. Notification Board, el cual mediante su uso permite a los módulos notificar entre si acerca de eventos que ocurren al interior de la red, eventos tales como cambios en las tablas de enrutamiento.

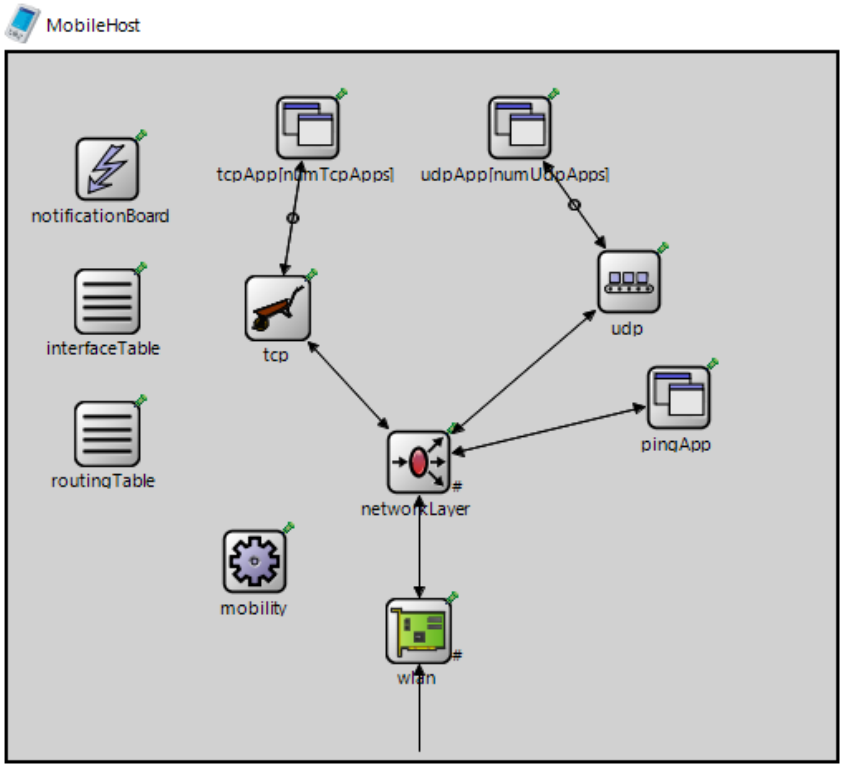


Fig. 10. Arquitectura del nodo MobileHost

b. Interface Table, la cual se encarga de la lógica de capa 2. Este módulo contiene propiedades de aquellos protocolos independientes a las interfaces.

c. Routing Table, que contiene los parámetros de reenvío de IPs (IpFowarding).

d. TCPApp, es la plantilla TCP para aplicaciones, la cual define los parámetros que una aplicación TCP necesita para que sea capaz de ser usada por un Host.

e. UDPApp, igual que TCPApp se comporta como la plantilla para aplicaciones definiendo los parámetros para una aplicación UDP.

f. TCP, es utilizado para la comunicación entre el protocolo TCP y aplicaciones clientes. Soporta todas las especificaciones del protocolo TCP, además de configuraciones de sockets.

g. UDP, que es la implementación del protocolo UDP para IPv4 e IPv6 y que puede ser conectado a varias/muchas aplicaciones.

h. PING App, que genera las solicitudes de ping y calcula la pérdida de paquetes y los parámetros de ida y vuelta de las respuestas.

i. NIC, que implementa una tarjeta de red con estándar 802.11 en modo ad-hoc. En su interior tiene submódulos los cuales son:

   - Ieee80211MgmtAdhoc, que se encarga de la administración del modo ad-hoc, es decir, del envío y recepción de tramas.
   - Ieee80211Mac, que implementa el protocolo MAC 802.11b y está hecho para ser usado en combinación con el módulo Ieee80211Radio como capa física.
   - Ieee80211Radio, se comporta como la capa física para el modelo 802.11. Incluye puertos para realizar la comunicación con las interfaces de los otros módulos.

j. Network Layer, que es la capa de red para un nodo IP. Contiene la configuración de las interfaces que transportan TCP, UDP, echo/ping, RSVP. En su interior encontramos implementados módulos para protocolos ICMP, IGMP, ARP y uno de errorHandling.

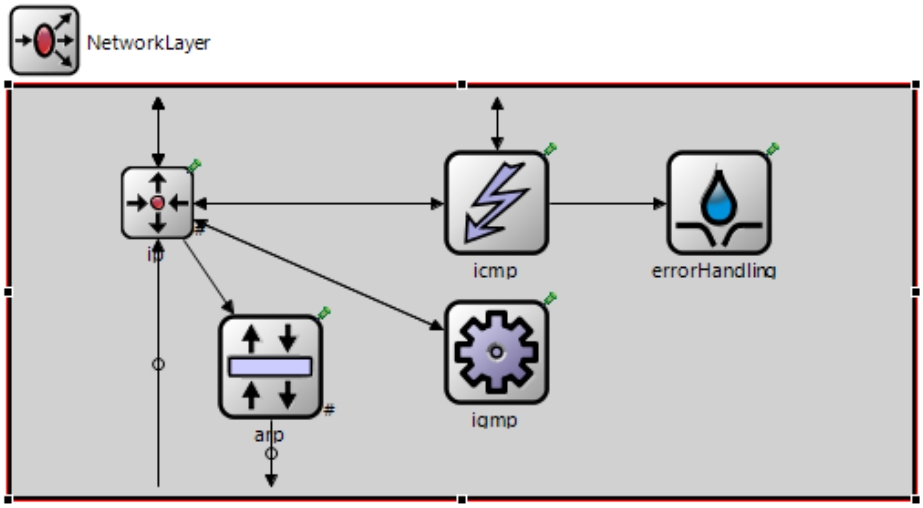


Fig. 11. Arquitectura de la capa de red

3.4. CONFIGURACIÓN DE OMNET

Para instalar y configurar OPNET debemos seguir los pasos:

- Descargar OMNeT + + 4.1 para Windows y descomprimirlo en “C:\”. Esto debe darle una secuencia de comandos “C:\mingwenv.cmd” que debe ejecutar para abrir una ventana de línea de comandos MinGW que se asemeja mucho a un entorno Linux.
- Construir OMNeT + + 4 ejecutando en la ventana de MinGV “./Configure” (asegurándose de examinar el resumen de los posibles errores). Si todo ha salido bien, esto se construirá el directorio en c:/omnetpp-4.1/bin/omnetpp.
- Ejecutar omnetpp para lanzar el OMNeT + + 4 IDE.

Luego de estos nos concentraremos en el framework INETMANET que nos servirá para definir la arquitectura VANET que vamos a simular. Para su instalación continuaremos con los siguientes pasos:

- Abrir el IDE e importar el proyecto INET (Archivo -> Importar -> General -> Proyectos existentes en el área de trabajo -> Seleccionar la ubicación del folder de inet -> Comprobar proyecto INET - Finalizar>
- Construir el proyecto con Ctrl-B.
- Crear un nuevo proyecto y se hacer referencia al framework INET.
  Archivo -> Nuevo -> OMNeT + + Proyecto de C + +
  Introducir un nombre y confirmar
- Abra las propiedades del proyecto de su nuevo proyecto, active la casilla INET en las referencias del proyecto y confirmar.

Al final podrá hacer uso de todas las características INET en su proyecto.

3.5. CRACKEO DE WEP CON AIRCRACK Y COMMVIEW PARA WIFI

3.5.1. CONSIDERACIONES

Para realizar el crackeo de una red con seguridad WEP o WPA debemos tener en cuenta las siguientes consideraciones:

a. Tener un equipo con una tarjeta de red que pueda ser colocada en modo monitoreo o promiscuo. Para este caso se hace uso de una tarjeta Dell 1397 cuyo chipset es compatible con nuestro programa de monitoreo, de manera que se pueda monitorear la red y capturar los paquetes encriptados que viajan a través de esta.
b. Utilizar un programa de monitoreo que administre la tarjeta de red inalámbrica y que pueda capturar los paquetes, en este caso se utilizará COMMVIEW para WIFI.
c. Hacer uso de un software de decriptación para el archivo que guarda la información de los paquetes encriptados y que han sido capturados por el software de monitoreo, en este caso se utilizará AIRCRACK.

3.5.2. CONFIGURACIÓN DE UNA RED CON SEGURIDAD WEP

Para la configuración de una red con seguridad WEP se hará uso de un Access Point inalámbrico Cisco DPC2325. En este se hacen las siguientes configuraciones:

- Tipo de encriptación: WEP con key de 64 bits
- Service Set Identifier (SSID): inSSIDer wlan
- Basic Service Set Indentifier (BSSID): 70:71:BC:2B:68:E1
- Canal: 11
- La clave de 64 bits en hexadecimal es **1CBE991A83** y corresponde al número 123456789123 en sistema decimal.

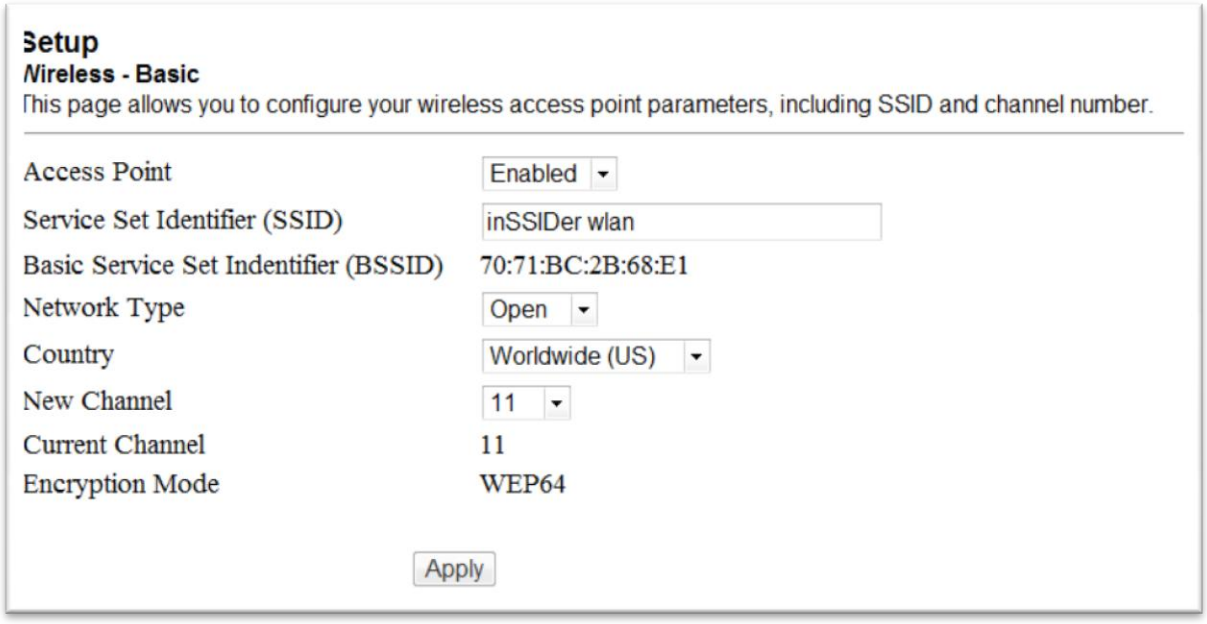


Fig. 12. Configuración de AP para red con seguridad WEP

3.5.3. UTILIZACIÓN DEL SOFTWARE DE MONITOREO COMMVIEW PARA WIFI

La instalación de COMMVIEW permite que se actualicen los driver de la tarjeta de red que permitirán colocarla en modo promiscuo. Luego de la instalación del software y si se instalaron correctamente los drivers de la NIC inalámbrica será posible ver el nombre de la tarjeta de red en la barra de títulos de COMMVIEW (ver figura 13).

Fig. 13. Identificación de NIC Inalámbrica.

Se continuará el procedimiento haciendo algunas configuraciones en el software que permitirán hacer una buena práctica.

Lo siguiente será ir a la pestaña de “Logging” y seleccionar la opción Auto-saving para configurar “Maximum Directory Size” y “Average Log File Size”, datos que nos permitirán definir el tamaño del archivo “log” y del directorio donde se encuentra; será suficiente con un tamaño de 100 MB para el archivo y 50000 para el directorio (ver figura 14).

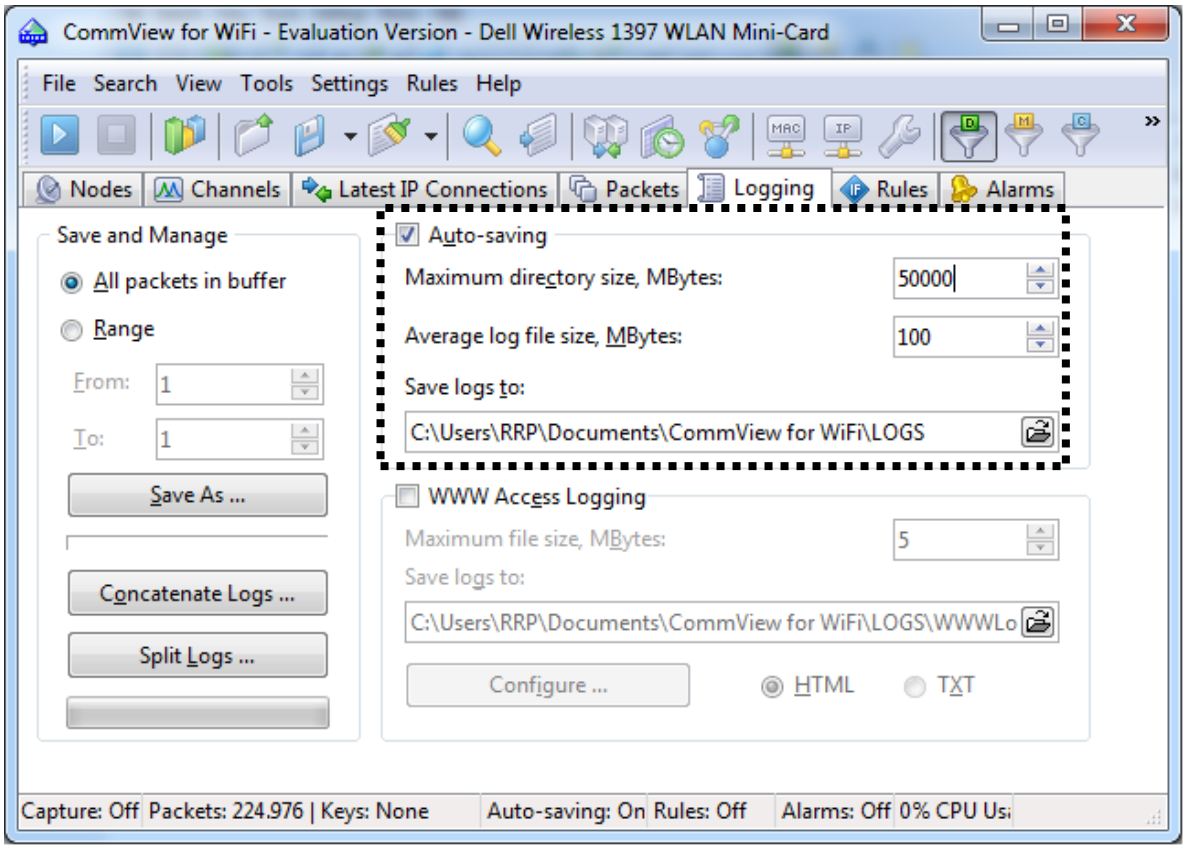


Fig. 14. Opciones de Auto guardado en COMMVIEW.

Ahora se debe seleccionar sólo la opción de captura de paquetes de datos, los cuales son los que llevan la mayor cantidad de IVs. Se debe omitir las opciones de lecturas de paquetes de administración y de control para que la captura de paquetes con IVs sea más certera (ver figura 15).

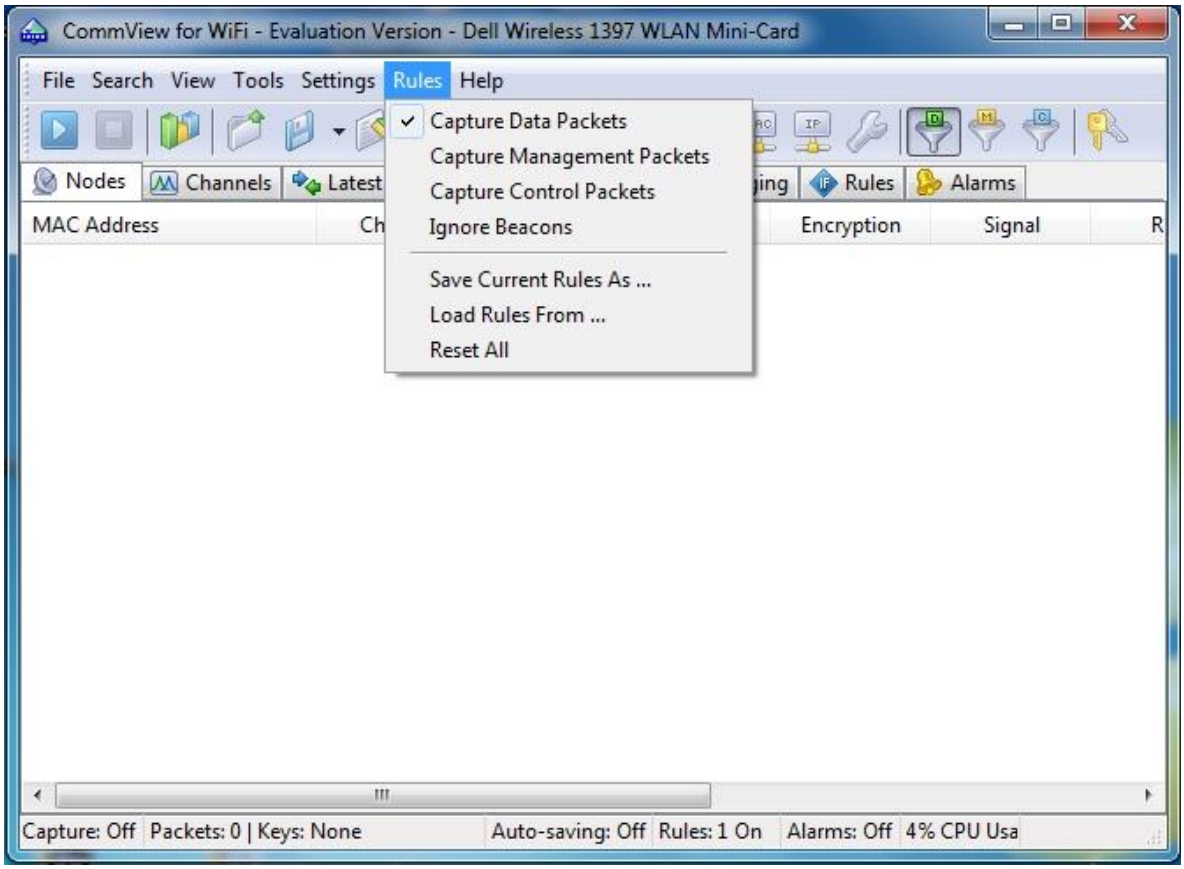


Fig. 15. Opción de captura de paquetes.

Luego de estas configuraciones iniciales procedemos a escanear la red en busca de canales que contengan nodos y conexiones con seguridad WEP para proceder a monitorearlas. Para ello se presiona en el botón “Iniciar exploración”, lo que hará visible en esta ocasión en el escáner dos dispositivos: el Access Point CISCO y el host como únicos nodos en esta red y que se encuentran en el canal 11 (ver figura 16).

Como siguiente paso se selecciona el Access Point con SSID “inSSIDer lan” cuyo identificador es Pegatron:2B:68:E1 y procedemos a capturar el trafico presionando el botón capturar.

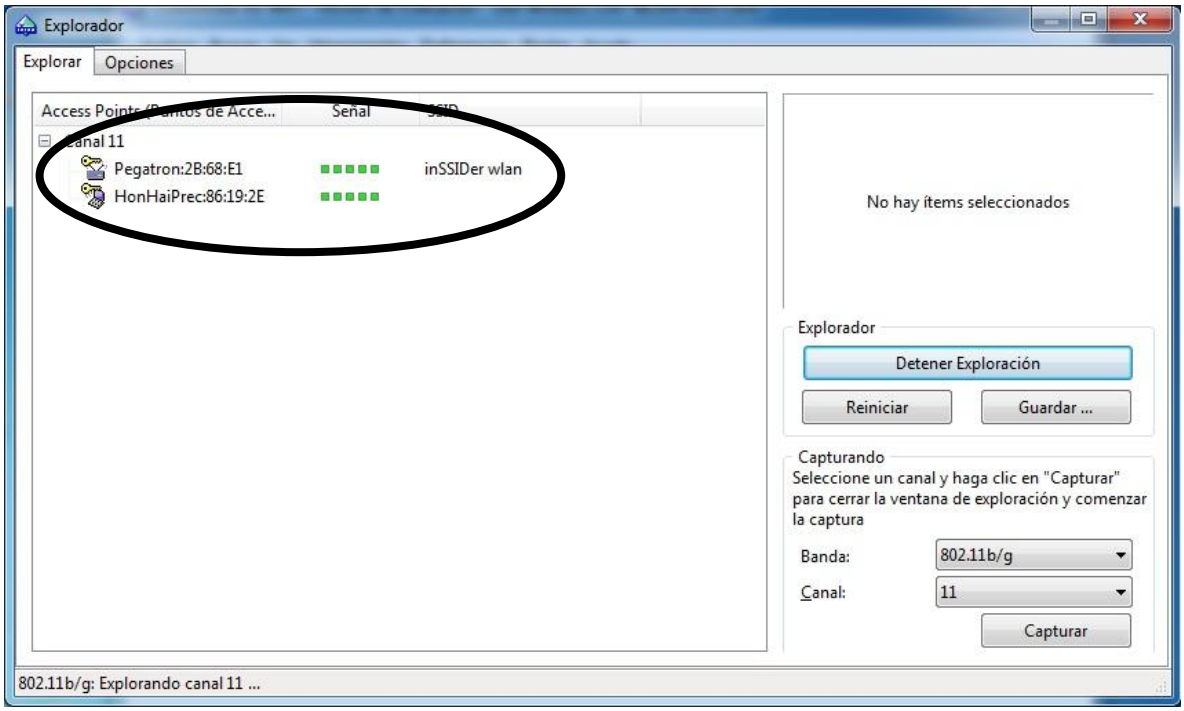


Fig. 16. Nodos de red con encriptación WEP.

Desde ya se empezarán a capturar paquetes que permitirán descubrir la clave WEP con la que se han encriptado. En la pestaña de canales “Channel” se podrá revisar el conteo de paquetes encriptados que han sido capturados, es recomendable que esperemos que este número se incremente hasta un poco más de 100.000 para asegurar la captura de por lo menos 5000 IVs para que sea posible y exitoso el proceso de decriptación (ver figura 17).

Fig. 17. Captura de paquetes encriptados.

Luego del proceso de captura procedemos a guardar el archivo con extensión .cap para que pueda ser reconocido por la herramienta AIRCRACK. Para esto se deberá realizar un último paso que será buscar el archivo log.ncf donde se encuentra la información de los paquetes capturados. Por defecto se encuentra en la carpeta c:\Users\usuario\documentos\commviewforwifi\logs\. Abrimos este archivo y luego se tendrá una ventana como la siguiente:

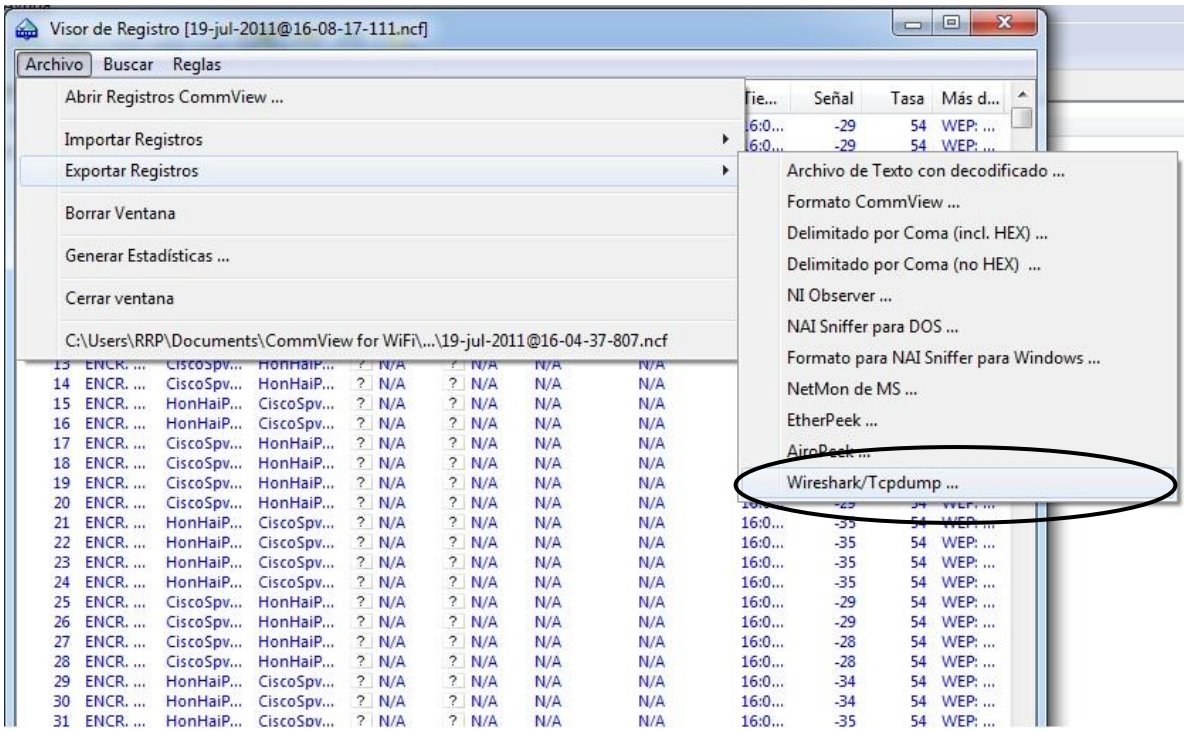


Fig. 18. Visor de archivo de captura.

3.5.4. UTILIZACIÓN DE AIRCRACK

Luego de haber realizado el procedimiento de monitoreo y captura de paquetes, se procederá a elegir el archivo generado *.cap en la herramienta AIRCRACK con el cual iniciemos el procedimiento de crackeo. Para esto debemos indicar opciones adicionales como el tipo de encriptamiento y el tamaño de la clave que se desea encontrar. En este caso será WEP de 64 bits como lo se había indicado inicialmente (ver figura 19).

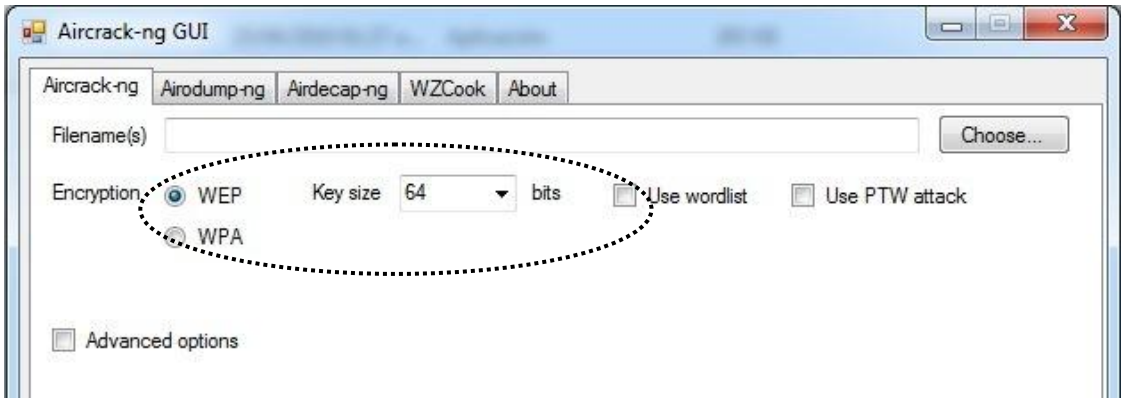


Fig. 19. Aircrack.

Presionando el botón launch se ejecutará AIRCRACK y se iniciará el proceso de desencriptación que terminará por encontrar la llave WEP utilizada para la autenticación en la red.

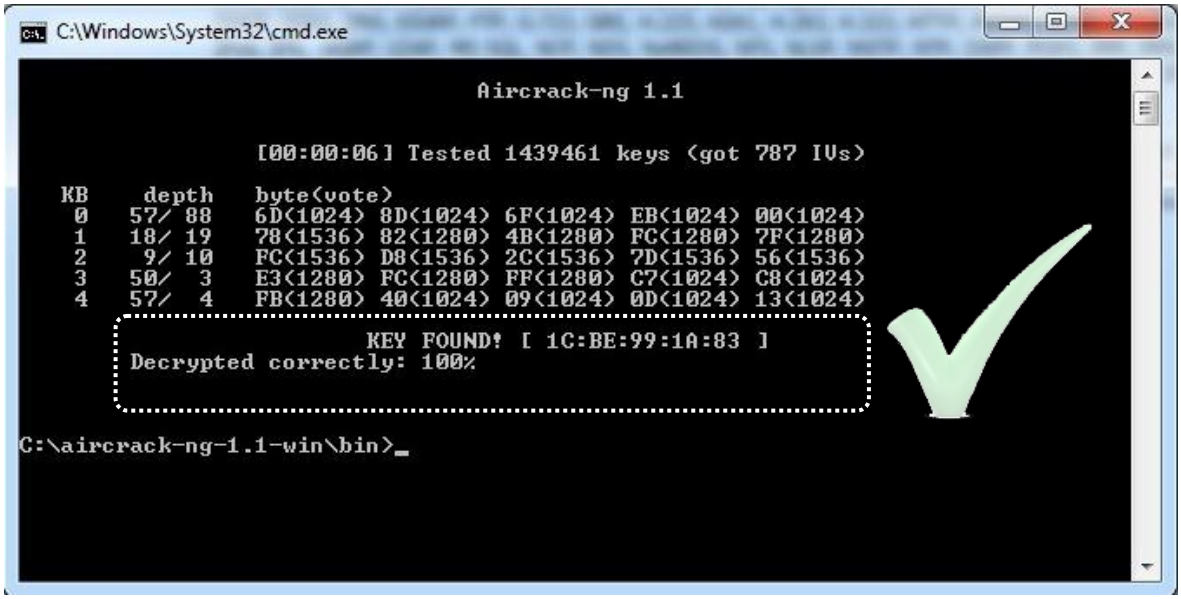


Fig. 20. Llave encontrada con Aircrack.

3.6. CRACKEO DE WPA CON AIRCRACK Y COMMVIEW PARA WIFI

El ejercicio de crackeo de llave WPA es similar al realizado para protocolo WEP. Las diferencias radican en el tipo de paquetes que debemos capturar para realizar el procedimiento de crackeo y algunas otras consideraciones adicionales que se deben tener en cuenta.

3.6.1. CONSIDERACIONES

a. Al igual que en WEP, se debe hacer uso de una NIC inalámbrica la cual pueda ser colocada en “MODO MONITOREO”, a través del uso de un software para este propósito.

b. Se debe también hacer uso de un software de monitoreo que permita escuchar y capturar tráfico de paquetes en la red que se quiere vulnerar.

c. Hacer uso de un software de crackeo para hallar la clave pre-compartida objetivo del ejercicio.

d. Adicional, se debe estar cerca físicamente del cliente que queremos atacar para así poder capturar paquetes específicos “handshake”, puesto que estos van directamente al cliente en el momento que se produce una des-autenticación. Esto si se quiere atacar en modo activo, es decir acelerar el proceso. De lo contrario restaría esperar a que un cliente intente conectarse al AP.

e. Se debe tener predefinido un “diccionario” con palabras que serían las posibles llaves pre-compartidas. Este es necesario para que AIRCRACK logre encontrar mediante una comparación la llave correcta.

f. Si se hace un ejercicio real donde no se conoce la víctima, y por tanto el diccionario debe ser extenso, se debe tener en cuenta la capacidad de procesamiento de la máquina, puesto que depende de esta el tiempo en el cual se logre dar con la posible llave. Este ejercicio puede durar semanas.

3.6.2. PROCEDIMIENTO

a. *Colocar la interface wireless en modo monitor y especificar el canal del AP.*

   El propósito de este paso es colocar la tarjeta en el modo denominado modo monitor. En este modo la tarjeta wireless puede escuchar y capturar cualquier paquete en el aire. En cambio, en el modo normal la tarjeta solo "escuchará" los paquetes que van destinados a la misma. Escuchando todos los paquetes, podremos más adelante capturar los 4 paquetes que forman el handshake WPA/WPA2. Y opcionalmente también podremos des-autenticar a un cliente wireless. Para lograr esto basta con iniciar el software COMMVIEW.

b. *Iniciar el escaneo y escucha de redes con seguridad para capturar el "handshake".*

   El propósito de este paso es ejecutar COMMVIEW para capturar los 4 paquetes del handshake en el momento que un cliente se autentifica con el AP en el que estamos interesados.

c. *Ejecutar AIRCRACK para obtener la clave pre-compartida.*

   El propósito de este paso es conseguir la clave WPA/WPA2 pre-compartida. Para hacer esto, se necesita un diccionario de posibles palabras. Básicamente, AIRCRACK comprueba cada una de esas palabras para mirar si coincide con la clave.

3.7. **ANÁLISIS DEL PROCEDIMIENTO DE CRACKEO EN WEP Y WPA.**

Por medio del ejercicio de crackeo se identificaron debilidades en los protocolos de control de integridad de la información WEP y WPA. Con respecto a WEP, quedo demostrado que en pocos pasos se puede descifrar la llave pre-compartida permitiendo tener acceso a la red. Para ello basto con capturar 100.000 paquetes transmitidos entre el cliente y el AP, los cuales fueron posteriormente analizados por AIRCRACK para descifrar dicha clave. Esto se debe a que el vector de inicialización se pueda reutilizar, lo que facilita los ataques puesto que dicha repetición garantiza que el atacante dispondrá de texto cifrado repetido para analizar.

WEP puede ser utilizado para redes domesticas donde la seguridad no es un tema critico, teniendo en cuenta que son necesarias pocas herramientas y alrededor de unos 10 minutos para vulnerar redes con este tipo de seguridad.

Referente al protocolo WPA, se puede decir que mediante un procedimiento de crackeo similar al usado en el protocolo WEP es posible descifrar la clave solo con algunas consideraciones adicionales. Para realizar este procedimiento no es necesario capturar demasiados paquetes, sino enfocarse en solo cuatro de estos que se encuentran en el flujo de red en el momento de autenticación entre cliente y AP. Estos paquetes son conocidos como 4-way handshake, los cuales contienen la clave encriptada de tamaño variable que va de 8 a 63 caracteres ASCII. Luego de la captura de estos cuatro paquetes se podrá realizar el procedimiento de crackeo, pero aun haría falta un diccionario de comparación que mediante múltiples pruebas de combinaciones pueda descifrar la clave. Sin embargo a pesar que de WPA es notablemente más seguro con respecto a WEP, es posible que se vulnere y no se constituye con una solución solida para el control de integridad de información en redes VANETS.

.

CONCLUSIONES

De acuerdo con la descripción y análisis de los protocolos, existen varias soluciones para la de seguridad para redes VANETS. La encriptación a nivel de capa de enlace es una medida comúnmente utilizada pero no garantiza confidencialidad, por lo que si se necesita seguridad se tiene que evitar el uso de WEP y pensar en utilizar WPA2.

Es recomendable utilizar el protocolo WPA2 para controlar la seguridad en redes VANETS, puesto que es mucho más seguro que WEP y WPA, los que fueron crackeados a través de AIRCRACK.

Es posible vulnerar WEP en pocos minutos teniendo el conocimiento y las herramientas necesarias, sin embargo para vulnerar WPA es necesario además mayor recurso de cómputo y tiempo.

Con un buen manejo de herramientas de análisis, monitoreo y crackeo de redes es posible vulnerar la seguridad de los protocolos de control de integridad.

Se describieron herramientas para modelar redes móviles, definiendo nodos y dispositivos en un escenario donde se pudieran interactuar y visualizar el comportamiento de estas. El uso de dichas herramientas permite alcanzar un mayor conocimiento y funcionamiento de este tipo de redes.

Los ejercicio de crackeo con las herramientas COMMVIEW y AIRCRACK, ratifican la vulnerabilidad del protocolo WEP y WPA, puesto que mediante un corto procedimiento se obtiene la clave de una red inalámbrica pre-compartida.

Las características de las redes VANETS hacen que sea difícil cumplir todos los requisitos de seguridad, sin embargo siguen siendo objeto de investigaciones, puesto se necesita proporcionar mecanismo de seguridad e integridad en estas redes.

GLOSARIO

- 802.11 – Estándar que define el uso de los dos niveles inferiores de la arquitectura OSI.
- 802.11i – Estándar implementado en WPA2, para especificar mecanismos de seguridad.
- 802.11x – Estándar Proporciona una autenticación mecanismo para dispositivos que deseen unirse a una red LAN o WLAN .
- AES - Advanced Encryption Standard, algoritmo de cifrado por bloques.
- APIs – Conjuntos de normas en los programas utilizar para poder comunicarse entre sí.
- ARP - Address Resolution Protocol, protocolo para traducir las direcciones IP a direcciones MAC.
- ATM - Modo de Transferencia Asincrónica. Es una tecnología de redes de alta velocidad que transmite múltiples tipos de información mediante la creación de paquetes de datos.
- BGP - Border Gateway Protocol, es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.
- BSSID - Basic Service Set Identifier, Dirección MAC del punto de acceso.
- C++ - es un lenguaje que abarca tres paradigmas de la programación: la programación estructurada, la programación genérica y la programación orientada a objetos.
- CCMP - Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol, protocolo de encriptación utilizado en WPA2, basado en la suite de cifrado de bloques AES.
- COMMVIEW – Herramienta para analizar y monitorear redes.
- CRACKEAR - Introducir un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio.

- CRC-32 - Cyclic Redundancy Check, pseudo-algoritmo de integridad usado en el protocolo WEP (débil).
- DARPA - Defense Advanced Research Projects Agency es una agencia del Departamento de Defensa de los Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar.
- DOCSIS - Data Over Cable Service Interface Specification Se trata de un estándar no comercial que define los requisitos de la interfaz de comunicaciones y operaciones para los datos sobre sistemas de cable.
- EDCA - Enhanced Distributed Channel Access.
- EIGRP - Enhanced Interior Gateway Routing Protocol,
- Ethernet - Estándar de red. Tipo de red de área local. Se apoya en la topología de bus; tiene ancho de banda de 10 Mbps.
- FDDI - Fiber Distributed Data Interface, es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica.
- Frame Relay - Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.
- Framwork - plataforma, entorno, marco de trabajo. Estructura de soporte definida, en la cual otro proyecto de software puede ser organizado y desarrollado.
- GNED - Detector mundial de Sucesos Nucleares.
- GUI - Componente de una aplicación informática que el usuario visualiza y a través de la cual opera con esta.
- HCF - Hybrid Coordination Function.
- HTTP – En inglés Hypertext Transfer Protocol. Protocolo de Transferencia de Hipertexto. HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información hipermedia.
- IEEE - Siglas en inglés para Institute of Electrical and Electronics Engineers, organización profesional internacional sin fines de lucro, para el avance de la tecnología relacionada a la electricidad.
- ICV - Integrity Check Value, campo de datos unido a los datos de texto para la

integridad (basado en el algoritmo débil CRC32).

- INET Framework - es un código abierto de comunicación paquete de simulación de redes para el OMNeT, contiene modelos de protocolos de red de varios cableadas e inalámbricas
- IP - Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet.
- IPv6 – es una versión del protocolo IP.
- IV - Initialization Vector, vector de inicialización, datos combinados en la clave de encriptación para producir un flujo de claves único.
- KEY STREAM - un flujo de clave es un flujo de azar o pseudo-personajes que se combinan con un texto mensaje para producir un mensaje cifrado.
- MAC - Es una dirección que usualmente está compuesta por números y letras asignado a los equipos que forman parte de una red, que es único e identifica su lugar dentro de la red.
- Mesh – red en malla implementada sobre una red inalámbrica.
- MIC - Message Integrity Code, campo de datos unido a los datos de texto para la integridad (basado en el algoritmo Michael).
- MPLS - Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar.
- MSDU - Mac Service Data Unit, paquete de datos después de la fragmentación.
- OLSR - Optimized Link State Routing.
- OPNET - Lenguaje de simulación orientado a las comunicaciones.
- OSPF - es un protocolo de enrutamiento jerárquico de pasarela interior.
- PING - Packet Internet Groper, este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa.
- PNNI - es un estado de enlace protocolo de enrutamiento utilizado en ATM redes.
- PSK - Pre-Shared Key, clave derivada de una frase de acceso que sustituye a la PMK normalmente enviada por un servidor de autenticación.
- QoS – concepto de calidad de servicio.

- QualNeT - es una simulación de la red herramienta que simula inalámbrica y por cable en modo paquete de redes de comunicación.
- RADIUS - Siglas del inglés Remote Authentication Dial In User Service. Está definido en RFC 2865, protocolo para la autenticación remota.
- RC4 – Algoritmo de cifrado de flujo más utilizado en el protocolo WEP, brindando seguridad en las redes inalámbricas.
- RIP - Protocolo de Enrutamiento de Información, protocolo de puerta de enlace interna.
- RSVP - Protocolo de reserva de recursos, es un protocolo de la capa de transporte diseñado para reservar recursos de una red bajo la arquitectura de servicios integrados.
- TCP - En español es Protocolo de Control de Transmisión y Protocolo de Internet.
- TD-CDMA – Interfaz de aire usada en nodos móviles.
- Tkenv – herramienta para diseñar gráficos de red de forma automática.
- TKIP - Temporal Key Integrity Protocol, protocolo de encriptación usado en WPA basado en el algoritmo RC4 (como en WEP).
- TSC - TKIP Sequence Counter, contador de repetición usado en TKIP.
- UMTS - Sistema Universal de Telecomunicaciones Móviles, es una de las tecnologías usadas por los móviles de tercera generación.
- VANETS – Redes vehiculares de acceso móvil.
- WEP - Wired Equivalent Privacy, protocolo de encriptación por defecto para redes 802.11.
- WIFI - Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz.
- WPA - Wireless Protected Access, implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP.
- WPA2 – versión mejorada de WPA.

REFERENCIAS

[1] Alberto Los Santos Aransay / Seguridad en Wi-Fi /Universidad de Vigo: Redes personales y locales. Artículo citado Julio de 2009. Web: http://www.albertolsa.com/wp-content/uploads/2009/07/alberto-los-santos-seguridad-en-wi-fi.pdf

[2] Oriol Batalla Alcalde/Seguridad en 802.11: Estudio y desarrollo de un sistema de gestión para EAP-TLS/Julio de 2009.
Web: http://upcommons.upc.edu/pfc/bitstream/2099.1/7488/1/PFC-OriolBatalla.pdf

[3] Guillaume Lehembre/ Seguridad Wi-Fi – WEP, WPA y WPA2/ Artículo publicado en el número 1/2006 de la revista www.hakin9.org

[4] Julio Cesar Ardita/ANALISIS DE WPA/WPA2 Vs WEP/ Escuela Politécnica del Ejercito-Ecuador/Publicado Febrero de 2008.
Web: http://www.cybsec.com/upload/ESPE_Analisis_WPA_WEP.pdf

[5] Saulo Barajas/Protocolos de seguridad en redes inalámbricas/Universidad Carlos III de Madrid. Web: http://www.saulo.net/pub/inv/SegWiFi-art.htm

[6] Vicent Alapont/Seguridad en redes inalámbricas/Universidad de Valencia/Web: http://documentos.shellsec.net/otros/SeguridadWireless.pdf

[7]CUEVA MENDOZA, Cesar Blademir. SEGURIDAD EN REDES INALÁMBRICAS. Universidad Nacional de Cajamarca. Febrero de 2010. Web:http://es.scribd.com/doc/26694435/SEGURIDAD-EN-REDES-INALAMBRICAS

[8] Martin Beck, Erik Tews/Practical attacks against WEP and WPA/8 de noviembre de 2008. Web: http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[9] Departamento de Ingeniería Telemática. Sección de Ingeniería Telemática de l'EPSEVG. Septiembre de 2004. Manual de Usuario de OPNET. Disponible en la Web: http://docente.ucol.mx/falberto_galvez/opnet.pdf

[10] María del Carmen Pastor Morales. Simulación en OPNET de ataques a la seguridad 802.11 mediante técnicas de jamming. Escuela Técnica Superior De Ingenierías Informática Y De Telecomunicación. Granada, 8 de julio de 2009. Web:http://tstc.ugr.es/it/pfc/proyectos_realizados/downloads/Memoria_CarmenPastor.pdf

[11] Deschamps Espinosa, Melissa Elena. Modelado de Mecanismos de Transición a IPv6. Universidad de las Américas Puebla. 17 de mayo de 2007. Web:http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/deschamps_e_me/capitulo4.pdf

[12]Miguel Andrés Alonzo, Carlos Bueno López. Simuladores UMTS. 2005. D. Web: http://trajano.us.es/~fornes/RSR/2005/UMTS/Simuladores%20UMTS%20-%202005.pdf

[13] Simulation whit OMNeT++.
Web:http://www.omnetpp.org/index.php/documentation/3632

[14] Scalable Network Technologies, Inc. Qualnet Simulator User´s Manual Version 3.1. Los Angeles, California, 90025. 2000, 2001. Web: http://www.eurecom.fr/~chenj/SimulatorManual-3.1.pdf

[15] Yuval Shavitt. Department of Electrical Engineering - Systems Department. Advanced Laboratory in Computer Communications. Basics of OPNET IT Guru Academic Edition. Web:http://www.eng.tau.ac.il/~netlab/resources/booklet/lab0.pdf

[16] Juan Agustín Zaballos, Cesc Canet. Security Labs in Opnet It Guru. Universidad Ramon Llull. Barcelona 2004. Web:http://www.ee.ui.ac.id/netlab/files/OPNET%20Security%20Lab%20Hands%20On/INTRO.pdf

[17] Javier Turegano Molina. Simulador NS-2. Marzo 2006. Web: http://linuxalbacete.org/web/index2.php?option=com_content&do_pdf=1&id=149

[18] Alfonso Roldán Bravo. Estudio de modelos de movimiento en interiores para aplicación en entornos WLAN. Universidad Politécnica de Cataluña. Diciembre 2007. Web: http://upcommons.upc.edu/pfc/bitstream/2099.1/4554/1/memoria.pdf

[19] Patxi Azpiroz De Pedro. Integración de Radio Mobile y NS-3 para la planificación de redes rurales híbridas WiMAX+WiFi. Universidad Carlos III de Madrid. Julio 2010. Web: http://www.ehas.org/uploads/file/difusion/academico/PFC/PFCradiomobile_ns3.pdf

ARTÍCULO CIENTÍFICO

Análisis de los protocolos de control de integridad Existentes en VANETs (Redes de Acceso Vehicular)

Carlos Mauricio Muñoz Ebratt1, Roberto Carlos Romero Payares2.

1Estudiante de Ingeniería de Sistemas de la Universidad Tecnológica de Bolívar
2Estudiante de Ingeniería de Sistemas de la Universidad Tecnológica de Bolívar

Abstract

Las redes inalámbricas presentan una serie de retos tecnológicos muy importantes al no tener infraestructura de red. Las redes Vanets se apoyan en las tecnologías actuales de redes inalámbricas, lo que se constituye en un problema debido al medio de comunicación y a las vulnerabilidades de los protocolos de integridad en esta topología de red. La falta de infraestructura para poder centralizar los servicios de seguridad, constituye un agravamiento en las Vanets. Analizando cada uno de los protocolos y sus aplicaciones, se pretende alcanzar mecanismos óptimos que permitan garantizar la integridad de los datos en este tipo de redes, donde la topología dinámica y la falta de un procesamiento centralizado hacen que alcanzar estos objetivos se una tarea más difícil. Un análisis crítico de los protocolos WEP, WPA, WPA2 y TKIP, en términos de fiabilidad e integridad nos permitirá hallar aquellas soluciones necesarias para la implementación de mecanismos adaptables a las Redes de Acceso Vehicular permitiendo así una consolidación de redes AdHoc confiables.

Keywords: *acceso, comunicación, protocolos, redes, seguridad, vehicular.*

Introducción

Una de las áreas de investigación más activas en tecnología automotriz de los últimos años es la de VANET (vehicular ad hoc network), cuyo objetivo es desarrollar plataformas de comunicación entre vehículos en movimiento y entre estos y la infraestructura vial. Para ellos se aprovecha las capacidades de

cómputo y comunicaciones inalámbricas con que cuentan actualmente los automóviles y las correspondientes capacidades que pueden obtenerse a través de la infraestructura vial.

La finalidad de una plataforma como ésta es incrementar la seguridad vial y la eficiencia de transporte, a la vez que reducir el impacto ambiental del tráfico vehicular. Debido a la importancia de sus objetivos, esta línea de desarrollo tecnológico está recibiendo especial atención a nivel mundial, lo mismo por parte de fabricantes de automóviles que de parte de los gobiernos.

Debido a todos los cambios tecnológicos generalizados en el ámbito de la seguridad en redes inalámbrica y por tanto en redes de acceso vehicular, se hace necesario hacer un análisis de la vulnerabilidad de los protocolos existentes, con el fin de direccionar una solución en la implementación de mecanismos que permitan garantizar la integridad de la información en este tipo de redes, es decir, el diseño de un protocolo de integridad propiamente dicho para estas redes. Actualmente se investiga muchísimo en este campo. Con el objetivo de establecer estándares abiertos en esta área emergente, la IETF [1] en castellano la Fuerza de Tareas de Ingeniería de Internet, creó el grupo de trabajo MANET [2] para estandarizar protocolos y las especificaciones funcionales de las redes ad hoc inalámbricas.

Con la intención de introducirnos en el análisis de los protocolos en el ámbito de la seguridad y por tanto integridad de los datos en las redes Vanets vamos a explicar en este artículo el tipo de tecnología implementada por dichas redes, las aplicaciones de estas y cada uno de los protocolos existentes hasta el momento.

Estado del Arte

I. Red de Área Vehicular – VAN

a. Definición

Las redes inalámbricas Ad hoc se denominan comúnmente como MANET, que es el acrónimo en inglés de Mobile Ad hoc Network. Las redes VANETs son un caso particular de las redes ad-hoc (Mobile Ad-hoc Network) enfocadas a entornos vehiculares. [3] Una red móvil Ad hoc es pues una colección de nodos móviles autónomos que se comunican entre sí mediante enlaces inalámbricos, sin la necesidad de utilizar un Punto de Acceso,

estableciendo conexiones punto a punto. Cada una de estas redes punto a punto se denominan Independent Basic Service Set (IBSS), y las conexiones tendrán un identificador propio denominado Independent Basic Service Set Identifier (IBSSID), posibilitando servicios de comunicaciones allí donde no existe una infraestructura de red fija ni administración centralizada.

b. Tecnologías

Tecnología IEEE 802.11

Más conocida como WiFi, se basa en el estándar IEEE 802.11. Opera en bandas libres. Las versiones b y g se han extendido mucho hasta el punto de que la mayoría de los equipos portátiles y PDAs la traen incorporada de serie. Tiene un alcance de unos centenares de metros y un ancho de banda de hasta 54 Mbps, dependiendo de la versión del estándar. La nueva versión, 802.11n pretende aumentar las tasas de transferencia hasta un 500Mps. La seguridad forma parte de los protocolos desde el principio y fue mejorada en la revisión 802.11i. [3]

Tecnología IEEE 802.11p

También conocida como Wireless Access for the Vehicular Environment (WAVE), es una evolución del estandar IEEE 802.11a con modificaciones a nivel físico y MAC para mejorar su comportamiento en el entorno vehicular y dar soporte a sistemas de transporte inteligente (Itelligent Transportation Systems (ITS)).Asimismo, WAVE es la base del desarrollo del DSRC (Dedicated Short Range Communications), otro proyecto de estandarización impulsado por el ministerio de transporte de EE UU y por un número importante de fabricantes de la industria automóvil, cuyo objetivo es crear una red nacional de comunicaciones vehiculares. [3]

II. Áreas de Aplicación

a. Seguridad activa: La seguridad es uno de los temas primordiales en el desarrollo de tecnología automotriz, razón por la que este grupo de aplicaciones de las VANET es el de mayor interés. Su objetivo es hacer más segura la conducción de vehículos mediante la comunicación oportuna de señales de advertencia sobre una posible colisión, una velocidad excesiva de arribo a una curva, fallas en las condiciones del vehículo (frenos, luces, tren motriz, etc.). Estas aplicaciones pueden emplearse, incluso, para permitir que el vehículo intente de forma automática evitar el accidente o para

que reaccione de la mejor manera, en caso de que éste sea inevitable.

b. Servicios públicos: Ejemplos sobresalientes de este tipo de aplicaciones es el apoyo que pueden obtener los vehículos de emergencia (ambulancias, policía y cuerpos de rescate) mediante “sirenas virtuales”, anunciadas con anticipación a los demás vehículos. El conductor puede, así mismo, ser advertido sobre una potencial infracción al reglamento de tránsito, por ejemplo, al entrar a una zona con límite de velocidad inferior a la actual o al anunciar vuelta en una zona no autorizada, etc.

c. Mejoras de conducción: Este tipo de aplicaciones pueden emplearse para que los vehículos avisen un cambio en sus condiciones de movimiento (reducción o incremento de velocidad, cambio de carril, etc.) o su localización a los otros vehículos cercanos; también es posible recabar información de la infraestructura vial sobre la velocidad óptima de llegada a un semáforo para coincidir con la fase verde, zonas de embotellamiento o la disponibilidad de lugares de estacionamiento o permitir el diagnóstico remoto del vehículo, etc.

d. Negocios y entretenimiento móvil: En este grupo se encuentran aplicaciones para facilitar la realización de transacciones durante el viaje, como pueden ser el pago de cuotas de peaje, descarga de contenidos multimedia, reservaciones, etc. [4]

III. Protocolos de Integridad

Ahora bien, con respecto a los protocolos de seguridad utilizados en las Redes de Acceso Vehicular, podemos señalar que son los mismos implementados en las redes inalámbricas debido a la naturaleza de las mismas. Estos protocolos de control de seguridad proporcionan integridad en el tráfico de los datos en términos de ciframiento y autenticación por parte de los usuarios (hosts).

a. Protocolos Existentes

- Wired Equivalent Privacy (WEP)

  WEP es un protocolo de seguridad para Wi-Fi de redes. Dado que las redes de transmisión inalámbrica de datos por ondas de radio, es fácil de interceptar los datos o "espiar" a las transmisiones de datos inalámbricos. El objetivo de WEP es hacer que las redes inalámbricas tan seguras como las

redes de cable. El protocolo de privacidad equivalente por cable añade seguridad a una red inalámbrica mediante la encriptación de los datos. Si los datos son interceptados, será irreconocible para el sistema que intercepta los datos, ya que se cifra. Sin embargo, autorizó a los sistemas de la red será capaz de reconocer los datos, ya que todos utilizan el mismo algoritmo de cifrado. Sistemas en una red WEP garantizado normalmente puede ser autorizado mediante la introducción de una contraseña de red. [5]

- Wi-Fi Protected Access (WPA)

WPA implementa la mayoría del estándar IEEE 802.11i y fue creado como una medida intermedia para ocupar el lugar de WEP mientras el propio estándar era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi), antigua Wireless Ethernet Compatibility

- Alliance (WECA).

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave "pre-compartida" (PSK: Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red. [6]

- Protocolo de Integridad de Clave Temporal – TKIP

TKIP o Protocolo Dominante Temporal de la Integridad (Temporal Key IntegrityProtocol), también conocido como hashing de clave WEP WPA, basado para brindar unamejor protección al protocolo WEP el cual puede ser quebrado de una manera fácil, con elalgoritmo que utiliza TKIP para encriptación de los datos se puede tener una red segura y sinla necesidad de cambiar de hardware para soportar otros protocolos.

El funcionamiento de TKIP se basa en generar una clave temporal (hashing), estamisma clave es compartida entre los equipos de la red inalámbrica y los puntos de acceso (AP), posteriormente TKIP utiliza el hashing y la MAC del cliente para combinarlos, así mismo le agrega la clave del vector de inicialización de 16 octetos generado y con esto cifra los datos, esta clave se

reemplazara después de cada 10,000 paquetes. Una de las cuestiones similares a WEP, es que TKIP utiliza RC4 para cifrar el mensaje. [7]

b. Análisis de los protocolos

- Wired Equivalent Privacy (WEP)

El principal problema radica en que no implementa adecuadamente el vector de iniciación del algoritmo RC4, ya que utiliza un enfoque directo y predecible para incrementar el vector de un paquete a otro. Además existe un problema con el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación. Conociendo los IV utilizados repetidamente y aplicando técnicas relativamente simples de descifrado puede finalmente vulnerarse la seguridad implementada. Aumentar los tamaños de las claves de cifrado aumenta el tiempo necesario para romperlo, pero no resulta imposible el descifrado. [8]

- Wi-Fi Protected Access (WPA)

WPA implementa un código de integridad del mensaje (MIC: Message Integrity Code), también conocido como "Michael". Además, incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo "Michael" fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, los drivers de las estaciones se desconectarán un tiempo definido por el fabricante, si reciben dos colisiones "Michael" en menos de 60 segundos, podrán tomar medidas, como por ejemplo reenviar las claves o dejar de responder durante un tiempo específico. [9]

- Protocolo de Integridad de Clave Temporal – TKIP

Ofrece mejoras significativas a la codificación de datos, lo cual incluye un método de reintroducción de clave, ofrece la mezcla de claves por paquete, la verificación de la integridad de los mensajes y un mecanismo de reintroducción de clave, el cual consta de un vector de inicialización o IV de 58 bits, una clave de 128 bits, generación de bloques de 4 Bytes (MIC) a partir de la dirección de origen, de destino y datos, es decir, cifra el checksum incluyendo direcciones MAC. [10]

Conclusiones

Las redes de acceso vehicular VANETS, han provocado la aparición de cantidad de grupos de investigación para afrontar el desarrollo de los servicios tradicionales que usamos en Internet. Se espera que estos grupo y sus investigaciones traigan consigo la evolución de los protocolos existentes y mejoras para el rendimiento de los dispositivos involucrados en redes VAN. La seguridad en estas redes es un aspecto de mucho cuidado debido a que los nodos pueden ser cualquier dispositivo, esto hace que el medio en que viajan los flujos de datos sea inseguro y se requieran mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad. En este artículo se ha identificado la tecnología con la cual trabajan las redes móviles, el área de aplicación y los protocolos de seguridad.

Referencias

[1] Internet Engineering Task Force

[2] IETF MANET Working Group: http://www.ietf.org/html.charters/manet-charter.html

[3] Estudio comparativo de protocolos de encaminamiento en redes vanet - Helene Doumenc, Universidad Politécnica De Madrid.

[4] Elmar Schoch et. al. Communication Patterns in VANETs. IEEE Communications - Magazine, Noviembre, 2008.

[5] Techterms.com

[6] http://www.ingeniatic.net/index.php/tecnologias/item/665-wifi-protected-access-wpa

[7]http://es.scribd.com/doc/52089734/65/PROTOCOLO-DOMINANTE-TEMPORAL-DE-LA-INTEGRIDAD-TKIP

[8]Seguridad en Wi-Fi, artículo de Alberto Los Santos Aransay

[9] http://www.ingeniatic.net/index.php/tecnologias/item/665-wifi-protected-access-wpa

[10]http://www.hacktimes.com/files/RompiendoElProtocoloWPAconPSKyTKIP-I.HackTimes.com.1.0.pdf