Estudio comparativo sobre simulación de escenarios de protocolos SAODV y AODV

Darwin Aguilar S.[a1], Paola León P.[a1], Diego Rojas R.[a]
{dlaguilar, rpleon1, dprojas}@espe.edu.ec

[a] Universidad de las Fuerzas Armadas – ESPE, Departamento de Eléctrica y Electrónica, , Av. Gral. Rumiñahui s/n, Sangolquí, Ecuador - P.O.BOX 171-5-231B.

[1]Grupo de Investigación de Propagación, Control y Networking (PROCONET)

Resumen. En las redes inalámbricas de tipo Ad-Hoc el protocolo AODV es el más eficiente en lo que se refiere a enrutamiento de paquetes debido a que se trata de un protocolo de tipo reactivo. Sin embargo un ámbito muy importante dentro de una red inalámbrica es la seguridad, lamentablemente el protocolo AODV no implementa ningún tipo de seguridad. AODV está diseñado para confiar en la red y confiar en cada una de las estaciones dentro de ella, es decir su creación asumía escenarios en donde se suponía no existen nodos maliciosos. Sin embargo y debido a las múltiples aplicaciones que actualmente se ejecutan y posiblemente a nuevos conocimientos de los usuarios esta falta de seguridad a obligado a trabajar con protocolos seguros como SAODV. El protocolo SAODV, implementa algoritmos de encriptación y cadenas hash con el fin de asegurar la integridad y confidencialidad de los datos que circulan a través de la red. En esta investigación se proponen escenarios simulados utilizando el software NS-2 (Network Simulator) mediante los cuales se comprueba la eficiencia y costo de red que implica el uso de SAODV frente a AODV.

Palabras Clave: SAODV, AODV, Ad-Hoc, Seguridad, Función Hash, Criptografía, NS2.

1 Introducción

Las redes Ad-Hoc nacen bajo el concepto de autonomía e independencia, al no requerir el uso de infraestructura pre-existente ni la necesidad de soportar su administración en esquemas centralizados como lo hacen las redes actuales, entre sus principales características podemos detallar las siguientes:

- Topología Dinámica
- Variabilidad del canal radio
- Usa tablas de enrutamiento
- No usan una infraestructura para su red
- Ancho de banda limitado
- Uso de Baterías

Una red Ad-Hoc al ser una red inalámbrica es vulnerable a distintas clases de ataques, como por ejemplo: espionaje mediante la inserción de nodos maliciosos, subversión de nodos, ataques de denegación de servicio, ataques de análisis de tráfico, ataque Sybil, ataques de replicación de nodos, ataques sinkhole, ataques wormhole. Dentro

del funcionamiento de las redes Ad-Hoc se han creado protocolos de encaminamiento activos como: AODV, DSR y reactivos como: OLSR. Estos protocolos también son vulnerables a estos tipos de ataques, sin embargo existen distintos requerimientos y planteamientos para implementar un nivel máximo de seguridad a las redes inalámbricas y específicamente a las redes Ad-Hoc, uno de los protocolos que propone implementar seguridad a una red Ad-Hoc es el protocolo SAODV.

2 Protocolo AODV

AODV (Ad hoc On-Demand Distance Vector) es un protocolo de tipo reactivo, es decir, solo busca rutas cuando un nodo necesita establecer comunicación con otro nodo, esta forma de funcionamiento evita generar sobrecarga de información innecesaria en la red.

Los mensajes que se envían desde los nodos origen no tienen información sobre el trayecto de la ruta, solo conocen el origen y el destino. AODV no mantiene rutas para cada nodo de la red. Estas rutas son descubiertas según se vayan necesitando bien sea que se activen o desactiven nodos en la red. AODV es capaz de proveer transmisión unicast, multicast y broadcast.

AODV permite la creación de tablas de enrutamiento en cada nodo para evitar transportar rutas en los paquetes. Cada destino de la tabla de enrutamiento lleva asociado un número de secuencia y un temporizador o ***lifetime***. Este número permite distinguir entre información nueva e información antigua, de tal manera que se evita la formación de lazos y la transmisión de rutas caducadas. Para un funcionamiento óptimo del protocolo AODV cada nodo debe mantener su número de secuencia actualizado. [1][6]

2.1 Descubrimiento de ruta

Para obtener la ruta necesaria para el envío de paquetes desde un nodo origen hacia un nodo distinto se toman en cuenta las siguientes consideraciones:

2.1.1 Camino de regreso

Cuando un nodo desea comunicarse con un nodo destino pero ignora cómo alcanzarlo envía un mensaje de petición (RREQ) de tipo broadcast, el mensaje contiene las direcciones IP y números de secuencia del origen y destino, Si un nodo no es el destino y desconoce la ruta hacia el destino entonces reenvía el mensaje a los siguientes nodos de la red hasta alcanzar al nodo destino. Este procedimiento es ilustrado en la Figura 1.

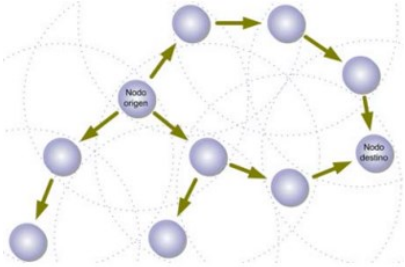

Fig. 1. Proceso de descubrimiento de ruta del protocolo AODV, en donde el nodo origen envía un mensaje REQ tipo broadcast a toda la red y forma un camino de regreso

2.1.2 Camino de ida

Cuando uno de los nodos ha recibido el mensaje de petición y este es el nodo destino o tiene una ruta para acceder al destino, envía un mensaje de repuesta de ruta (RREP). El mensaje (RREP) se envía de forma unicast desde el destino hacia el origen copiando el mismo camino de los mensajes (RREQ). La Figura 2. Nos muestra gráficamente el proceso de descubrimiento de la ruta y la Figura 3, ilustra la selección de ruta cuando existe más de una alternativa válida.

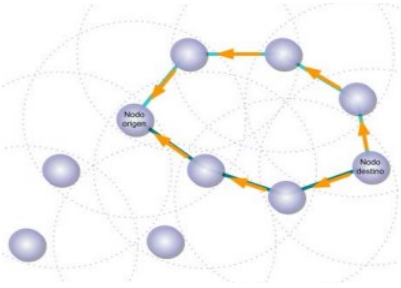

Fig. 2. Proceso de descubrimiento de ruta del protocolo AODV, en donde el nodo destino envía un mensaje REP tipo unicast a los nodos que solicitaron la ruta.

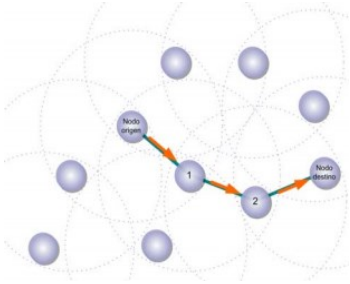

Fig. 3. El nodo origen examina las dos rutas posibles para llegar al destino y elige la que contiene el menor número de saltos.

2.1.3 Mantenimiento de Ruta

La función principal del mantenimiento de rutas en el protocolo es el de informar a un nodo origen cuando un enlace falle, de esta manera puede buscarse una nueva ruta. Por ejemplo si un nodo intermedio cambia de posición, este deberá informar a todos sus vecinos que necesitan de esta estación para transmitir. El mensaje de cambio, se lo envía al resto de nodos (saltos) y la ruta antigua será eliminada.

Para detectar la falla de un enlace el protocolo AODV utiliza los mensajes HELLO, estos mensajes son enviados periódicamente por todos los nodos hacia sus vecinos para anunciar su presencia en la red, si un nodo deja de recibir un mensaje HELLO de algún vecino puede considerar que el enlace con dicho vecino ha dejado de operar, e inmediatamente envía un mensaje de error de ruta (RERR) a sus vecinos y estos a su vez lo envían a los nodos que tengan rutas relacionadas con el nodo afectado. Adicional cuando el nodo origen recibe el mensaje de error de ruta puede iniciar nuevamente el proceso de descubrimiento de ruta. [2]

2.1.4 Vulnerabilidades

El protocolo AODV no implementa ningún tipo de seguridad, está diseñado para confiar en la red y confiar en cada una de las estaciones dentro de ella, es recomendado para escenarios en donde se considera que no existen nodos maliciosos.

3 Protocolo SAODV

El protocolo SAODV (Secure Ad hoc On-Demand Distance Vector), que es una extensión del protocolo AODV, que se utiliza para proteger el descubrimiento de ruta, mecanismo que proporciona características de seguridad como integridad y autenticación. Se utiliza dos mecanismos para asegurar los mensajes AODV: firmas digitales para autentificar los campos que no son mutables de los mensajes y el las cadenas hash para asegurar la información del número de saltos (el único campo que se modifica en los mensajes). Para obtener la información no mutable, la autenticación es realizar de una manera de extremo a extremo, pero el mismo tipo de técnicas no se puede aplicar a la información mutable.

La información relativa a las cadenas hash y las firmas se transmite con el mensaje AODV como un mensaje de extensión (vamos a referirnos a ella como la extensión de la firma).

3.1 Requerimientos de seguridad que satisface

Dentro de las características principales que implementa el protocolo SAODV, tenemos a los mecanismos de seguridad desarrollados en los algoritmos de firmas y cadenas hash, en los cuales se incluyen propiedades de integridad, autenticación y confidencialidad. [3]

3.1.1 Autenticación

Cada nodo de la red Ad-Hoc es capaz de comprobar si un nodo es quien dice ser, esta información la puede comprobar mediante un identificador y la firma que posee cada nodo en la red.

3.1.2 Integridad

La integridad consiste en verificar si la información que sale desde un nodo origen es la misma que llega a un nodo destino, es decir comprueba que no exista ningún tipo de alteración en la información.

3.1.3 Confidencialidad

La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona que la genera. Para esto las cadenas de hash se utilizan para crear firmas de un solo uso que pueden ser verificados inmediatamente. El principal inconveniente de este uso es la necesidad de sincronización de reloj.

3.2 Cadena Hash

SAODV utiliza cadenas de hash para autenticar la cuenta de saltos de los mensajes RREQ y RREP generados, de tal manera que permite a cada nodo que recibe estos mensajes (ya sea un nodo intermedio o el destino final) verificar que el salto recuento no ha disminuido por un atacante. Esto evita un ataque de replicación de nodos (por ejemplo). Una cadena de hash se forma mediante la aplicación de una función hash unidireccional varias veces para un nodo inicio. Cada vez que un nodo se origina un RREQ o un mensaje de RREP, se realiza las siguientes operaciones:

- Genera un número aleatorio (origen).
- Establece el campo Número de Max Hop al valor TimeToLive (del IP encabezamiento).

  Max_Hop_Count = TimeToLive

- Establece el campo de Hash para el valor de inicialización.

  Hash = inicio

- Establece el campo de función hash al identificador de la función hash que va a utilizar.

  Hash_Function = h

- Calcula Top Hash numerando los nodos inicio Max Hop Count veces.

$$Top\_Hash = h^{Max\_Hop\_Count}(inicio)$$

Dónde:
- h es una función hash.
- h^i (x) es el resultado de aplicar la función h a x i veces.

Además, cada vez que un nodo recibe una RREQ o un mensaje de RREP, se realiza las siguientes operaciones con el fin de verificar el número de saltos:

- Se aplica la función hash h Maximum_Hop_Count menos las veces Hop_Count a el valor en el campo de hash, y se verifica que el valor la resultante es igual al valor contenido en el campo Top_Hash.

$$Top\_ Hash == h^{Max\_Hop\_Count - Hop\_Count}\ (Hash)$$

Dónde:
- a == b lecturas: para verificar que A y B son iguales.

- Antes de la retransmisión de un RREQ o reenviar un RREP, se aplica un nodo la función hash al valor Hash en la extensión de la firma para la cuenta del siguiente salto.

$$Hash = h\ (Hash)$$

El campo Hash función indica que la función de hash tiene que ser utilizado para calcular el hash. Si intenta usar una función hash diferente, simplemente crear un hash mal sin dar ninguna ventaja a un nodo malicioso. Hash_Function, Max_Hop_Count, Top_Hash, y los campos hash se transmiten con el mensaje AODV, en la prolongación de la firma, pero el campo de hash se firmará para proteger su integridad.

3.3 Firmas Digitales

El proceso de descubrimiento de rutas del protocolo AODV permite responder a los nodos intermedios con un RREP, si tienen en su tabla de enrutamiento una ruta nueva hacia el destino haciendo de esta manera eficiente este tipo de protocolo, sin embargo, es más difícil implementar seguridad, ya que un nodo intermedio puede almacenar varias rutas en el proceso de descubrimiento de reversa después de recibir un RREQ de tal manera no podrá contar con la firma única para el RREP.

Para solventar este inconveniente el protocolo SAODV, ha creado dos tipos de soluciones que se detallan a continuación:

Si un nodo intermedio no puede firmar de manera correcta el mensaje de respuesta de ruta RREP entonces actuará como un nodo que no tiene la ruta en su tabla y continuará reenviando el RREQ a sus vecinos. La otra alternativa es que cada que un nodo crea un RREQ introduzca banderas, la firma y el tamaño de prefijo pueden ser usados por cualquier nodo intermedio que origine una ruta reversa al recibir un RREQ y para saber el nodo origen que origino el RREQ.

Por otro lado cuando un nodo intermedio genera un RREP el campo de tiempo de vida va a cambiar, entonces este nodo tendrá que generar el nuevo tiempo de vida e incluir los dos tiempos, el anterior que servirá para comprobar la firma del destino y adicional firmará el nuevo tiempo de vida, con esto se consigue que la información original sea firmada por el destino y el nuevo tiempo de vida por el nodo intermedio.

4 Simulador NS-2

Ns2 (Network Simulator) es una herramienta que nos brinda la posibilidad de simular escenarios de redes, además de ser un software con gran nivel de detalle, permite visualizar el funcionamiento de los protocolos de una manera completa. Ns2 permite obtener los resultados mediante archivos de traza gráfica de las variables que pueden ser aplicadas a los distintos escenarios que el usuario plantee. [4]

4.1 Network Animator (NAM)

NAM es una herramienta fundamental que utiliza NS2 ya que nos permite visualizar la simulación en tiempo real pudiendo observar los nodos de la red, la posición, el movimiento, el flujo de tráfico en la red, esto con el fin de mejorar la comprensión del funcionamiento de las redes y los protocolos de enrutamiento.

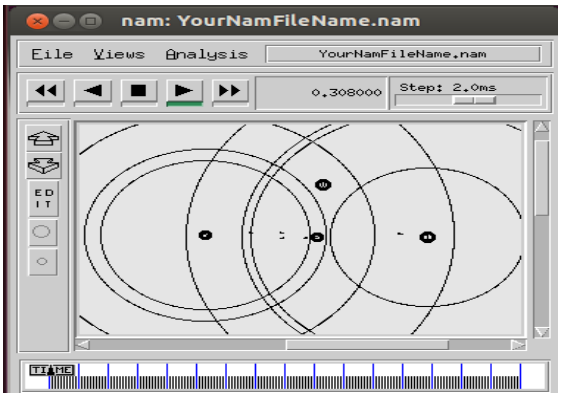

Fig. 4. Herramienta NAM que nos permite visualizar de forma gráfica el funcionamiento de la red en tiempo real.

4.2 Xgraph

La herramienta Xgraph que viene en NS2 nos sirve para interpretar los archivos de trazado y mostrarlos de forma gráfica. Dentro de los scripts TCL se debe agregar algunos comandos para realizar la interpretación del Xgraph.

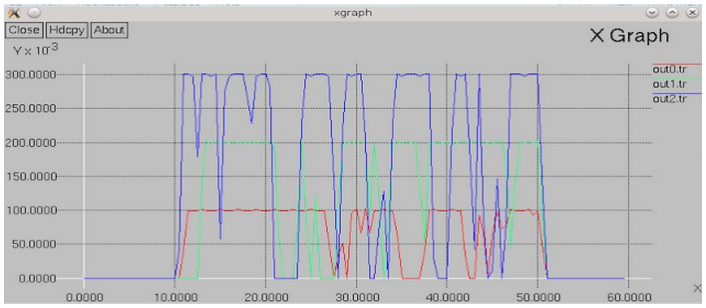

Fig. 5. Herramienta xgraph permite visualizar los resultados de la simulación en forma gráfica.

5 Escenarios

En el presente trabajo se diseñó 2 escenarios. El escenario A en donde se añade un nodo malicioso dentro de la red, el protocolo SAODV lo detecta y lo aísla descartando todos los paquetes que lleguen a él y evitando que lleguen a su destino. También se pone en funcionamiento el protocolo AODV el mismo que no es capaz de detectar el nodo malicioso y por ende todos los paquetes que llegan al nodo malicioso siguen su trayectoria hacia su destino.

En el escenario B se implementa seguridad a los mensajes del protocolo AODV, esto se lo realiza mediante algoritmos de un valor hash que garantiza la integridad de los datos y algoritmos de encriptación que protegen la confidencialidad. Este tipo de mecanismos de seguridad lo realiza el protocolo SAODV, de igual manera se pone en funcionamiento el protocolo AODV sin ningún tipo de seguridad para realizar la comparación entre los distintos parámetros de la red.

5.1 Consideraciones Escenario A

5.1.1 Topología

La topología propuesta es una red con 6 nodos ubicados arbitrariamente de forma tal que permita observar el intercambio de paquetes entre el origen y destino.

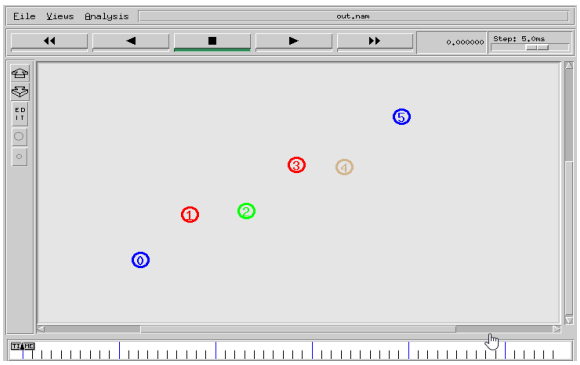

Fig. 6. Topología del escenario A que cuenta con 6 nodos ubicados de manera arbitraria para visualizar el intercambio de paquetes.

5.1.2 Modelos de conexión

Para inyectar tráfico a la red existen 2 tipos de paquetes (TCP y UDP) y con ellos sus respectivas aplicaciones que van a viajar junto a los paquetes de tráfico (FTP y CBR), para configurar el tipo de tráfico que se desea que exista en la red se debe modificar el script TCL como se indica a continuación:

```
set tcp0 [new Agent/TCP]
$ns attach-agent $n(0) $tcp0
set tcp1 [new Agent/TCP]
$ns attach-agent $n(1) $tcp1
set tcp2 [new Agent/TCP]
$ns attach-agent $n(2) $tcp2
set tcp3 [new Agent/TCP]
$ns attach-agent $n(3) $tcp3
set tcp4 [new Agent/TCP]
$ns attach-agent $n(4) $tcp4
set tcp5 [new Agent/TCP]
$ns attach-agent $n(5) $tcp5
```

Fig. 7. Configuración script TCL

5.1.3 Funcionamiento Protocolo AODV

Los paquetes se generan desde el nodo (0) que es el origen, llegan al nodo malicioso nodo (1) y este continua transmitiendo al resto de la red. [5]

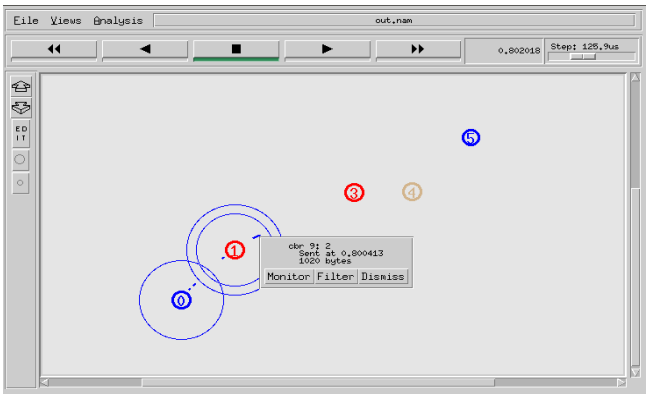

Fig. 8. Funcionamiento del protocolo AODV, los paquetes pasan por el nodo malicioso y se dirigen al destino.

Los paquetes CBR han llegado a su destino el nodo (5) desde el origen nodo (0)

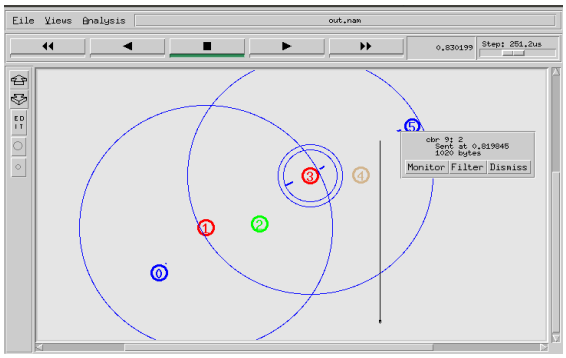

Fig. 9. Los paquetes llegan a su destino con un número de identificación, tiempo en el que se envió y el tamaño de los paquetes en bytes.

5.1.4 Funcionamiento Protocolo SAODV

El nodo malicioso es el nodo (1). El protocolo SAODV comparará su número de identificación con los números de los nodos que se encuentran registrados en la red y como no pertenece entonces lo aísla de la red y descarta todos los paquetes que llegan hacia él.

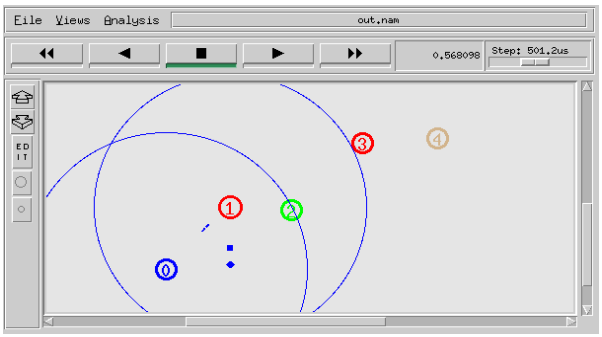

Fig. 10. Funcionamiento del protocolo SAODV, todos los paquetes que llegan al nodo 1 son descartados.

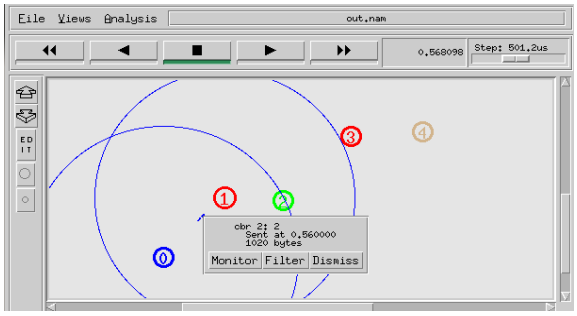

Fig. 11. Los paquetes antes de ser descartados llegan al nodo malicioso con un número de identificación, tiempo en el que se envió y el tamaño de los paquetes en bytes.

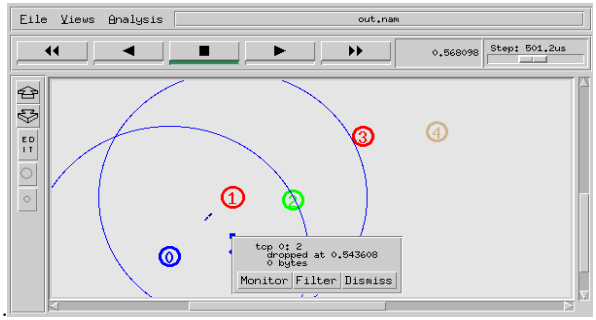

Fig. 12. Los paquetes después de ser descartados ya no cuentan con un número de identificación, tiempo en el que se envió y tampoco tamaño de los paquetes.

5.1.5 Archivos de traza

El archivo de traza nos indica cómo se comporta la red, en este archivo se puede visualizar todas las rutas que toman los paquetes para llegar hacia su destino, nodos origen, fuente, número de secuencia, tipo de paquetes, tamaño de paquetes, direcciones MAC, puerto origen, puerto destino entre otros parámetros de una red,

para generar un archivo de traza se ingresa los siguientes comandos en el script TCL: [7]

```
set wireless_tracefile [open normal.tr w]
$ns trace-all $wireless_tracefile
```

5.2 Consideraciones Escenario B

5.2.1 Topología

Para el escenario B se ha implementado seguridad en los mensajes AODV, por lo tanto no existe una topología definida como en el escenario A, a continuación se observa el funcionamiento del protocolo AODV que intercambia mensajes sin ningún tipo de protección.

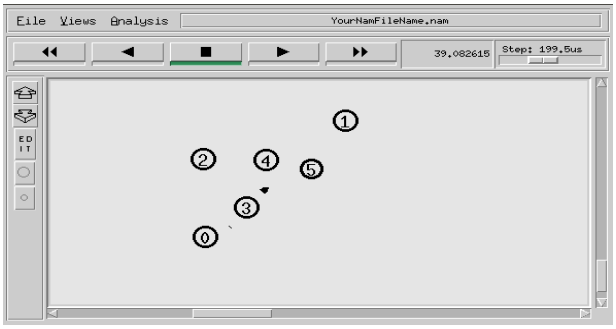

Fig. 13. Funcionamiento AODV, intercambio mensajes sin ningún tipo de protección.

Se generan 4 agentes Security_Packet en el script TCL, estos fueron creados mediante programación para que implementen seguridad a un paquete AODV. Cada agente está asociado a un nodo, por ejemplo el agente p0 se asocia al node_(0) y así sucesivamente con el resto de nodos y al finalizar se realiza la conexión entre los agentes que participarán en el intercambio de mensajes encriptados dentro de la red.

```
set p0 [new Agent/Security_packet]
$ns_ attach-agent $node_(0) $p0
$p0 set class_ 1
set p1 [new Agent/Security_packet]
$ns_ attach-agent $node_(1) $p1
$p1 set class_ 1
set p2 [new Agent/Security_packet]
$ns_ attach-agent $node_(4) $p2
$p2 set class_ 2
set p3 [new Agent/Security_packet]
$ns_ attach-agent $node_(5) $p3
$p3 set class_ 2
#Connect the two agents
$ns_ connect $p0 $p3
```

5.2.2 Funcionamiento Protocolo AODV

Se puede visualizar que los paquetes que llegan al nodo destino son TCP generados por el protocolo AODV, por ejemplo el paquete TCP #4775 es enviado a los 39.09 segundos de haber iniciado la simulación

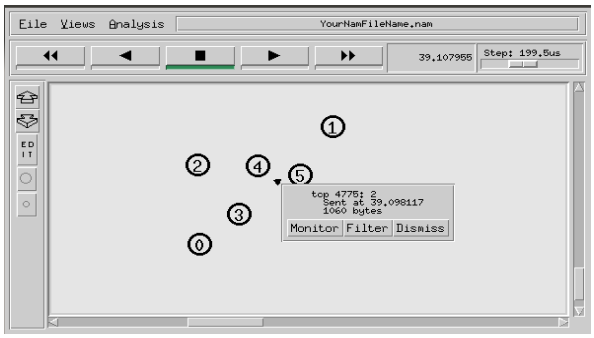

Fig. 14. Los mensajes intercambiados cuentan con todos los detalles de su transmisión, no se observa ningún mecanismo de seguridad.

5.2.3 Funcionamiento Protocolo SAODV

En el segundo evento ya actúa el protocolo SAODV que implementa seguridad a los paquetes AODV mediante un algoritmo de cadena hash y adicional la encriptación de los mensajes.

```
user1@ubuntu:~/Desktop$ ns packet_s.tcl
num_nodes is set 6
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Starting Simulation...
Message sent itisalongmessageIcansend with hashing 541705348
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
data intergity ensured
node 5 received packet from  0 with trip-time 9.8 ms - contend: lwlvdorqjphvvdjh
Lfdqvhqg - decrypted itisalongmessageIcansend -hash: 541705348
node 0 received packet from  5 with trip-time 11.7 ms - contend: Message_Accepte
d - decrypted _ -hash: 0
Message sent Itisashotermessage with hashing 9128228
Message sent test3 with hashing 406
Message sent test4 with hashing 486
data intergity ensured
node 0 received packet from  5 with trip-time 1.6 ms - contend: whvw7 - decrypte
d test4 -hash: 486
node 5 received packet from  0 with trip-time 3.4 ms - contend: Message_Accepted
 - decrypted _ -hash: 0
NS EXITING...
user1@ubuntu:~/Desktop$
```

Fig. 15. Funcionamiento del protocolo SAODV, se implementa los algoritmos de protección para proteger la confidencialidad y la integridad de los mensajes.

5.2.4 Archivo de traza

Mensaje encriptado enviado desde el nodo origen hacia el destino

```
s 0.009183380 _0_ MAC  --- 0 Security_packet 78 [13a 5 0 800] ------- [0:1 5:1 30 5]
r 0.009807684 _5_ MAC  --- 0 Security_packet 20 [13a 5 0 800] ------- [0:1 5:1 30 5]
```

Fig. 16. Archivo de traza del protocolo SAODV

El nodo destino recibe el mensaje del origen y envía un mensaje de confirmación

```
s 0.009832684 _5_ RTR  --- 1 Security_packet 20 [0 0 0 0] ------- [5:1 0:1 30 0]
s 0.011008292 _5_ MAC  --- 1 Security_packet 78 [13a 0 5 800] ------- [5:1 0:1 30 0]
r 0.011632596 _0_ MAC  --- 1 Security_packet 20 [13a 0 5 800] ------- [5:1 0:1 30 0]
r 0.011657596 _0_ AGT  --- 1 Security_packet 20 [13a 0 5 800] ------- [5:1 0:1 30 0]
```

Fig. 17. Archivo de traza del protocolo SAODV

6 Análisis de Resultados

Los resultados son analizados individualizando cada uno de los escenarios que fueron simulados:

6.1 Escenario A

6.1.1 Delay

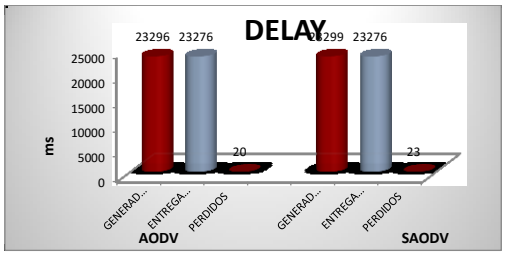

Fig. 18. Comparación retraso entre protocolos, SAODV no tiene retraso ya que todos los paquetes del nodo malicioso son descartados y nunca llegan a su destino.

6.1.2 Throughput

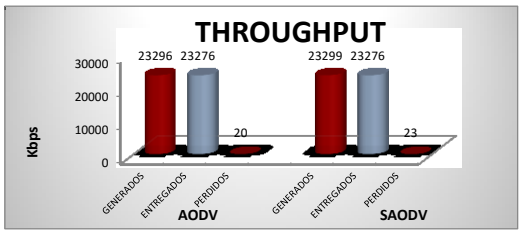

Fig. 19. Comparación del throughput entre los protocolos, el protocolo SAODV no genera ningún tipo de throughput por descartar todos los paquetes del nodo malicioso

6.1.3 Overhead

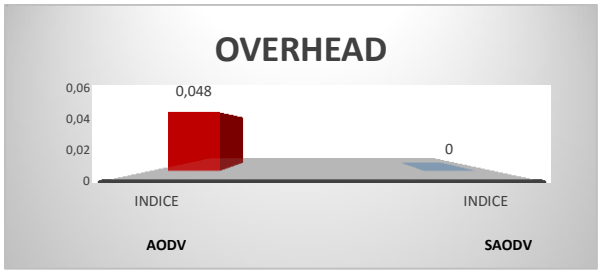

Fig. 20. Comparación de la sobrecarga entre los protocolos, el protocolo SAODV no produce sobrecarga en la red en este escenario ya que solo descarta paquetes

6.1.4 Ratio

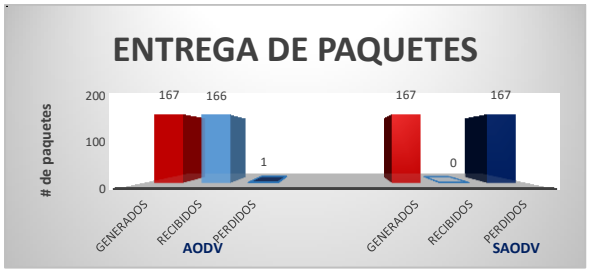

Fig. 21. Comparación de la tasa de entrega de paquetes entre los protocolos, de todos los paquetes generados ninguno llega a su destino en el protocolo SAODV

6.2 Escenario B

6.2.1 Delay

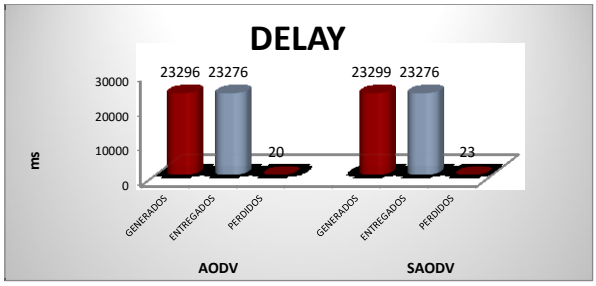

Fig. 22. El retraso en el protocolo SAODV es mayor debido a los paquetes de seguridad que se implementan, estos llegan al destino y se calcula el valor hash y desencripta el paquete.

6.2.2 Throughput

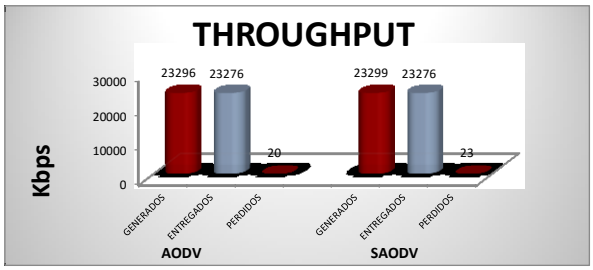

Fig. 23. En protocolo AODV la cantidad de datos reales de información que se transmitan en el flujo de la red serán un poco mayor que el protocolo SAODV.

6.2.3 Overhead

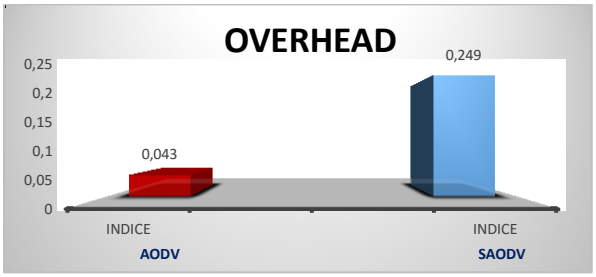

Fig. 24. La sobrecarga es mayor en el protocolo SAODV que en AODV, ya que además de contar con los bytes de control propias del protocolo AODV también se adicionan los bytes de seguridad propios del protocolo SAODV para verificar la integridad de un paquete.

6.2.4 Ratio

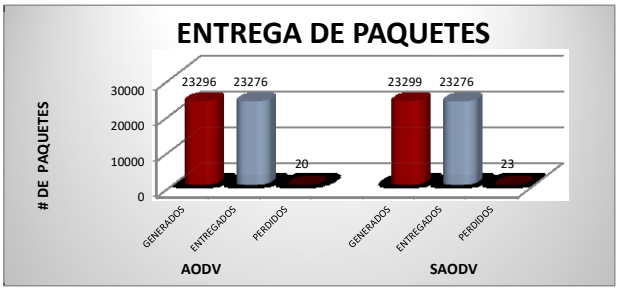

Fig. 25. La entrega de paquetes en ambos protocolo es casi similar, eso es debido a que el protocolo SAODV solo aplica mecanismos de seguridad al protocolo AODV sin cambiar el algoritmo de enrutamiento que el protocolo AODV utiliza, por eso evitará que se pierdan el menor número de paquetes en la transmisión.

7 Discusión y Trabajos futuros

Al implementar algoritmos de seguridad se sufre cierta sobrecarga y aumenta el nivel de procesamiento en los equipos por lo que es indispensable contar con equipos con nivel de procesamiento óptimo para no causar retardo en el envío de paquetes, también es importante implementar algoritmos de consumo de energía en los nodos cuando estos se encuentran sin actividad (modo sleep) ya que al momento de poner en funcionamiento la red deben estar al 100% para un óptimo funcionamiento, adicional se debería revisar la velocidad de transferencia de mensajes entre los nodos dependiendo el radio de transmisión, cuando un nodo vecino se encuentra cerca no debería transmitir el mensaje en la misma velocidad que un nodo que se encuentre fuera del radio de cobertura, con esto se reduciría un porcentaje de sobrecarga y nivel de procesamiento en la red.[8]

El protocolo SAODV no cubre todos los aspectos de seguridad que pueden ser vulnerados en una red como por ejemplo ataques por denegación de servicio que se sufre en la capa física por lo que se debe tener en cuenta este aspecto para trabajos futuros. [9]

Se debe aclarar que el protocolo SAODV no soluciona completamente el problema de seguridad del protocolo AODV ya que pueden existir ataques en la capa física en donde el protocolo no puede actuar, en lo que nos ayuda el protocolo SAODV es en implementar confidencialidad e integridad a los mensajes AODV.

Con la implementación del algoritmo de cadenas hash del protocolo SAODV es complicado que un nodo malicioso quiera involucrarse en la red ya que los nodos cuentan con un número de identificación que solo saben los verdaderos integrantes de la red, al momento de realizar el proceso de descubrimiento de ruta un nodo malicioso puede enviar mensajes REQ al resto, pero mensajes con información de tipo TCP serán descartados y no llegarán al nodo destino.

Se debe considerar el tipo de escenario en el que se va a desenvolver una red Ad-Hoc, para escenarios en el que se asume participan nodos confiables el protocolo AODV realizará un trabajo excelente sin mucha sobrecarga ni retardo en la red, pero si la red inalámbrica se lleva a cabo en un ambiente abierto entonces el protocolo SAODV es el indicado, ya que los más importante en una red es la seguridad, sin embargo existirá un poco más de retardo, sobrecarga y procesamiento de los equipos en la red debido a los algoritmos de seguridad que implementa, esto sin embargo es justificable con el fin de proteger la confidencialidad de nuestros datos.

Al momento de analizar el throughput se verifica que los dos protocolos trabajan casi de manear similar transmitiendo la misma cantidad de información en determinado tiempo, así que en cuestión de rendimiento ambos protocolos nos brindan similares características.

En el caso de la tasa de entrega de paquetes se verifica que ambos protocolos intentar evitar que se pierdan la menor cantidad de paquetes en una transmisión, los dos utilizan un mismo principio al momento de realizar el enrutamiento de los paquetes lo que garantiza que la mayoría de paquetes transmitidos llegarán a su destino, aunque el protocolo SAODV tardará un poco más en su entrega, lo transportará de una manera segura, característica que el protocolo AODV no aplica. [10]

En términos generales el protocolo SAODV es un protocolo eficiente al momento de brindar seguridad a una red Ad-hoc, posee cambios en ciertos parámetros comparados con el protocolo AODV, sin embargo no son cambios significativos que afecten el funcionamiento general de la red, tomando en cuenta que el protocolo SAODV brinda un aspecto muy importante en toda clase de red que es la seguridad.

Referencias

1. Peral, Alberto. Estudio del rendimiento y la seguridad en redes Ad Hoc (año 2014).
2. Calderón, Oscar, Seguridad en redes ad hoc (año 2011).
3. Diseño social-inspirado de la máquina virtual distribuida (örbis virtüalis maqüinus övm) para la red AD-HOC TLÖN (Colocom 2015 memorias).
4. Peterson – Davie, Network Simulation Experiements Manual (año 2012)
5. Bonastre, Oscar .Introducción a la programación de protocolos de comunicaciones con Network Simulator (año 2004).
6. Gil, María Elena, Estudio de la eficiencia de encaminamiento del protocolo AODV en redes ad hoc inalámbricas de gran escala (año 2009).
7. Ros, Francisco, Evaluación de Propuestas de Interconexión a Internet para Redes Móviles Ad Hoc Hibridas (año 2004).
8. Gómez, CarIes, Redes Ad-Hoc Próximo reto (año 2004).
9. Wister, Miguel, Arquitectura de descubrimiento de servicios en MANET basada en dispositivos de capacidades superiores liderando clusters (año 2008).
10. Zapata, Manel, Secure Ad hoc On Demand Distance Vector (SAODV) Routing (año 2005).