Ataque de Inundación en Redes Ad Hoc

1.- Introducción

La red móvil ad hoc es un sistema autónomo de nodos móviles conectados por ligas inalámbricas. Cada nodo no sólo opera como un fin de sistema, también como un router para retransmitir los paquetes. Los nodos son libres moverse y se organizan ellos mismos en una red. Las redes móviles ad hoc no requieren una infraestructura fija tales como estaciones base, además, es una opción atractiva para tener una red de dispositivos móviles de forma rápida y espontánea, tal como aplicaciones militares, operaciones de emergencia, dispositivos de red electrónicos personales y aplicaciones civiles como un salón de clases. Las redes ad hoc móviles tienen varias características sobresalientes, como son, las topologías dinámicas, la capacidad reducida de ancho de banda, capacidad variable en las ligas, debido a estas características, las redes móviles ad hoc son particularmente vulnerables a ataques por negación de servicio lanzado por un nodo intruso.

Las redes ad hoc móviles son desplegadas a menudo en ambientes dónde los nodos son desatendidos y tienen pequeña o ninguna protección física contra manipulaciones. Los nodos de las redes móviles ad hoc son así susceptibles a estar en peligro. Las redes son particularmente vulnerables a ataques de rechazo del servicio (DOS) lanzados por intrusos. Se presentará un nuevo ataque de DOS y su defensa en las redes ad hoc. El nuevo ataque de DOS, llamado “Ataque de Inundación en Redes Ad Hoc”, produce la negación de servicio cuando se están usando protocolos de ruteo bajo demanda para redes Ad Hoc, tales como AODV y DSR. El intruso transmite excesivos paquetes RREQ o envía muchos paquetes de DATOS para agotar el ancho de banda entre las comunicaciones y los recursos en los nodos, para que las comunicaciones válidas no puedan llevarse a cabo. Después de analizarse dicho ataque (ataque de inundación en redes Ad Hoc), se ha desarrollado una defensa genérica llamada Prevención al Ataque de Inundación (Flooding Attack Prevention, FAP). El FAP está compuesto de la supresión de vecino y corte de ruta. Cuando el intruso transmite paquetes "Route Request (RREQ)", los vecinos inmediatos del intruso observan una tasa alta de RREQ enviados por el atacante, entonces ellos bajan la prioridad de acuerdo a la tasa de RREQ entrantes, en pocas palabras la prioridad de un nodo va a ser inversamente proporcional a los paquetes RREQ que envía dicho nodo. Las peticiones de prioridad baja son eventualmente descartadas. Cuando el intruso envía muchos paquetes de DATOS al nodo víctima, el nodo puede cortar el camino y no volver a aceptar una ruta con el intruso. El ataque de inundación de redes Ad Hoc puede ser evitado fácilmente con FAP.

2.- Resumen del protocolo de ruteo AODV

En AODV, el descubrimiento de rutas es completamente contra-demanda. Cuando un nodo fuente necesita enviar paquetes a un destino al cual, no tiene ninguna ruta válida, el nodo transmite un paquete RREQ (Petición de Ruta) a sus vecinos. Cada nodo mantiene un único y creciente número de secuencia para asegurar rutas fuera de loops. El nodo fuente incluye el número de secuencia que conoce del destino en el paquete RREQ. El nodo intermedio recibe el paquete RREQ y verifica en las entradas de su tabla de ruteo si posee una ruta hacia el destino con un número de secuencia mayor que en el paquete de RREQ, si lo tuviese manda un paquete RREP (Contestación de Ruta) hacia el nodo fuente, a través de sus vecinos por los que recibió el paquete de RREQ. Por otra parte, si no tuviese un número de secuencia actual para el nodo destino, añade en su tabla de ruteo una entrada indicando que ya sabe como llegar a la fuente que generó el RREQ (camino inverso) y entonces retransmite el paquete de RREQ a sus vecinos. Los paquetes RREQ duplicados recibidos por un nodo son tirados. De esta manera, el paquete RREQ se inunda en una forma controlada en la red, y llegará eventualmente al destino mismo o a un nodo, el cual contenga una ruta actualizada en su tabla de ruteo, cualquiera de los dos generará un paquete RREP y lo mandará hacia la fuente por la misma ruta por la que le llego el RREQ. AODV también incluye el mecanismo de mantenimiento de ruta para manejar la topología dinámica de la red. Las ligas

que se rompen pueden ser detectadas ya sea por beacons periódicos o acknowledgments de la capa de enlace, tal como aquéllos proporcionados por el protocolo 802.11 MAC. Una vez que una liga está rota, un no solicitado paquete RRER con un número de secuencia actual y un número de saltos finito es propagado a todos los nodos fuentes activos, los cuales estén actualmente usando dicho link. Cuando el nodo fuente recibe la notificación de que una liga está rota, puede reiniciar la ruta con el proceso de descubrimiento de ruta, esto es si aun esta interesado tener dicha ruta hacia el destino.

3.-Ataque de inundación RREQ

La inundación de paquetes RREQ en toda la red consume muchos recursos. Para reducir la congestión en una red, el protocolo de AODV adopta algunos métodos. Un nodo no puede originar más de RREQ_RATELIMIT mensajes RREQ por segundo. Después de transmitir un RREQ, un nodo espera por un RREP. Si para dicha ruta no se recibe el RREP dentro de "round-trip" milisegundos, el nodo puede intentar descubrir la ruta de nuevo transmitiendo otro RREQ, a un máximo de intentos al valor de TTL máximo. Repetidos esfuerzos por un nodo fuente al descubrimiento de ruta para un solo el destino debe utilizar un "binary exponential backoff". La primera vez un nodo fuente transmite un RREQ, él espera un tiempo "round-trip" para la recepción de un RREP. Si un RREP no se recibe dentro de ese tiempo, el nodo fuente envía un nuevo RREQ. Al calcular el tiempo de espera para el RREP después de enviar el segundo RREQ, el nodo fuente debe usar un "binary exponential backoff". Por lo tanto, el tiempo de espera por el RREP correspondiente al segundo RREQ es 2 * round-trip time. Los paquetes RREQ son transmitidos en un anillo creciente reduciendo el overhead causado por la inundación de la red entera. Los paquetes se inundan en una área pequeña (un anillo) primero definido por un TTL inicial (tiempo-de-vida) en la cabecera IP. Si no se ha recibido el RREP, el área inundada se agranda aumentando el TTL por un valor fijo. El procedimiento se repite hasta que un RREP se reciba por el creador del RREQ, es decir, la ruta se ha encontrado.

El Ataque de Inundación en redes ad hoc, el nodo atacante viola las reglas anteriores para agotar los recursos de la red. Primeramente, el intruso selecciona muchas direcciones IP que no están en la red, esto es, si él sabe el alcance de direcciones IP en la red. Porque ningún nodo puede responder los paquetes de RREP para éstos RREQ, la ruta inversa en la tabla de ruteo del nodo será conservado mucho tiempo. El atacante puede seleccionar al azar las direcciones IP si es que él no puede saber alcance de las direcciones IP. Después, el atacante origina masivamente mensajes RREQ para estas direcciones IP nulas. El atacante intenta enviar RREQ's sin considerar un RREQ_RATELIMIT por segundo. El atacante reenviara paquetes RREQ sin esperar por el RREP o round-trip time. El TTL de los RREQ's se inicializan al máximo sin usar el método de expansión de anillo. En los ataques de inundación, la red entera estará llena de paquetes RREQ que el atacante envía. El ancho de banda de la comunicación es agotada por la inundación de paquetes RREQ así como los recursos en los nodos. Por ejemplo, el almacenamiento de la tabla de ruteo es limitada. Si masivos paquetes de RREQ están llegando a un nodo en poco tiempo, el almacenamiento en la tabla de ruteo del nodo se agotará y éste no podrá recibir nuevos paquetes RREQ. Como resultado, los nodos legítimos no pueden no descubrir rutas para enviar datos. La figura 1 muestras un ejemplo de un ataque por inundación de paquetes RREQ. El nodo H es el atacante e inunda con paquetes RREQ toda la red para que otros nodos no puedan construir rutas.

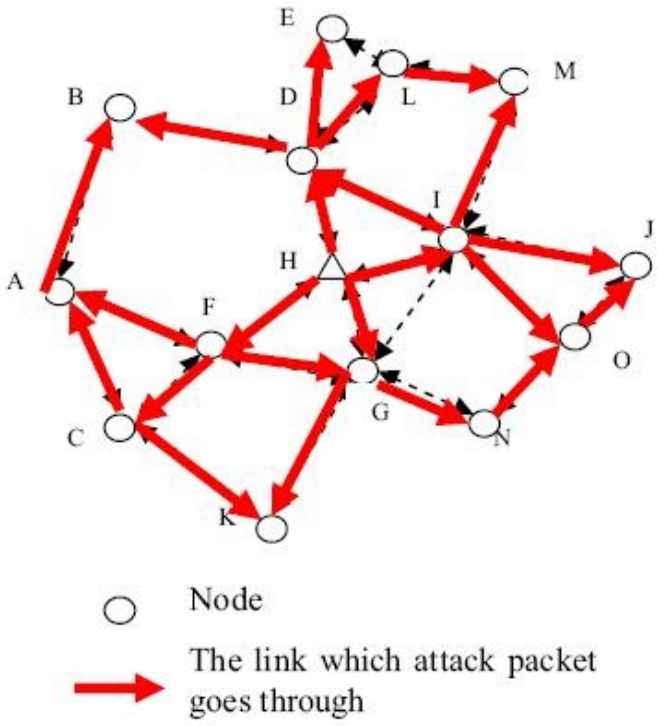

Figure1. The RREQ Flooding Attack

4.- Ataque por inundación de datos

Primero, el atacante crea rutas a todos los nodos en la red. Después, manda excesivamente paquetes de datos inútiles a través de dichas rutas. Los excesivos paquetes de datos en la red agotan el ancho de banda disponible para las comunicaciones entre los nodos. El nodo destino estará ocupado recibiendo los paquetes y no podrá trabajar normalmente.

La característica común de dos tipos de ataques de inundación es agotar el ancho de banda disponible de la red afectando así la comunicación legítima. Por otra parte, cada ataque tiene sus características particulares. El ataque por inundación de paquetes RREQ produce desbordamiento en la tabla de ruteo del nodo para que el nodo no pueda recibir nuevos paquetes RREQ. En el ataque de inundación de paquetes de DATOS, el proceso de recibir el ataque de paquetes consumirá muchos recursos en los nodos. Si el atacante combina dos tipos de ataques, producirá el colapso de la red entera.

5.- Comparación entre ataques de inundación en redes Ad Hoc y SYN

El ataque de inundación aprovecha el mecanismo de “tree-way handshake” de TCP/IP y su limitación en mantener conexiones entre-abiertas. Cuando un servidor recibe una petición SYN, éste regresa un paquete SYN/ACK al cliente. Hasta que el paquete SYN/ACK es reconocido por el cliente, la conexión se mantiene en un estado entre abierto por un periodo hasta que se llega a un timeout. El cual es típicamente de 75 segundos. El servidor ha construido en su sistema de memoria una cola para mantener todas las conexiones entre-abiertas. Desde que esta cola es de tamaño finito, una vez que ha alcanzado

su límite, todas las demás peticiones a conexión serán rechazadas. Si una petición SYN es alterada, el servidor victima nunca recibirá el paquete ACK final para completar el “tree-way handshake”.

Name	SYN Flooding Attack	Ad Hoc Flooding Attack
Attack method	TCP connection requests with spoofed source addresses	Flooding mass RREQ and DATA packets
Victim	host	Mobile ad hoc networks
Protocol	TCP/IP	On-demand routing protocol
Protocol layer	Transport layer	Network layer
goal	Denial of service in host	Denial of service in the whole networks

6.- Eliminación de vecinos

El método de eliminación de vecino es usado para prevenir el ataque por inundación de paquetes RREQ. Las redes móviles Ad Hoc son redes inalámbricas multi-salto, y los nodos mandan y reciben paquetes a través de sus nodos vecinos. Si todos los nodos vecinos alrededor de un nodo se rehúsan a retransmitir sus paquetes, el nodo no se podrá comunicar con los otros nodos en la red ad hoc, aislándose así de la red.

La figura 2 muestra una topología de red ad hoc móvil. El nodo H se comunica con los otros nodos a través de los nodos D, F, G e I. Si los nodos vecinos D, F, G e I se negasen a recibir paquetes del nodo H, el nodo H no podrá enviar ningún paquete a los otros nodos.

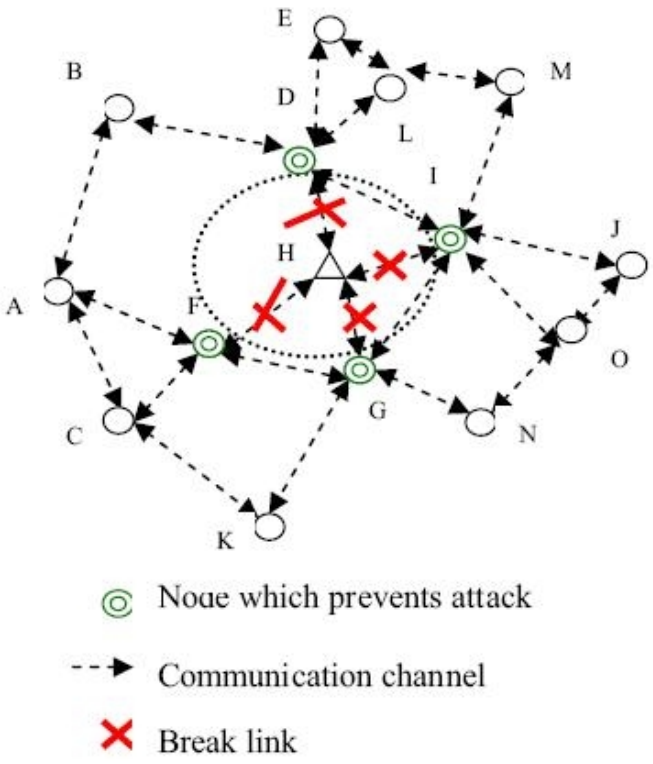

Figura 2. Neighbor node isolate attacker

En AODV, los nodos colocan los paquetes RREQ de acuerdo a la regla “first-in, first-out” (FIFO). Con dicha regla, los excesivos paquetes RREQ del atacante harán que se sature la cola y los nodos no podrán recibir los paquetes RREQ posteriores. Se cambiara la cola FIFO por una cola de prioridad. Además se tendrá un umbral de paquetes que se podrán recibir por cada vecino.

La prioridad de un nodo es inversamente proporcional a la frecuencia que origina RREQ. El umbral es el número máximo de paquetes RREQ que origina un nodo en un periodo determinado, tal como 1 seg. Si la frecuencia de originar RREQ del atacante excede el umbral, su vecino no recibirá más RREQ del atacante. Así como entre mas paquetes RREQ mande menor será su prioridad en la cola.

Para clarificar, tomamos el nodo F y sus vecinos A, C, H, G de la figura 3. El nodo F prepara el proceso de prioridad para sus vecinos A, C, H, y G. Los valores iniciales de las cuatro prioridades en el nodo F son 1's. Después del nodo A transmite dos paquetes RREQ en 1 segundo, la prioridad del nodo A cambia a 1/2. Si el nodo C origina 5 paquetes RREQ en 1 segundo, la prioridad del nodo C se cambia a 1/5. Después de esto, si el nodo A y C transmiten paquetes RREQ al mismo tiempo, el nodo F primero transmitirá el paquete RREQ del nodo A porque la prioridad de A es más alta que de C. Si el nodo H (intruso) transmite excesivamente paquetes RREQ en un período de tiempo, la prioridad de H será muy baja. Si la frecuencia excede el umbral, nodo F negará la retransmisión de los paquetes RREQ de H, esto es semejante, para el nodo D, I, G. Como resultado, será cancelado el ataque por inundación de RREQ por medio de los vecinos.

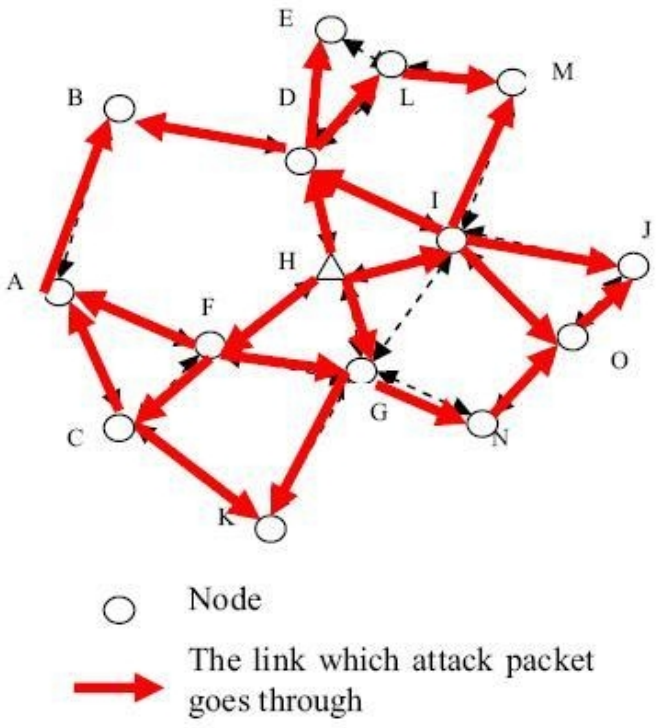

Figura 3

7.- Corte de ruta

Cuando el intruso origina un ataque de inundación de datos; para los nodos vecinos es difícil identificarlo, ya que no pueden juzgar que un paquete de datos es inútil en la red. Pero el nodo destino puede fácilmente determinar en la capa de aplicación cuando recibe un paquete de datos inútil. Se presentará un método llamado "corte de ruta" para prevenir el ataque por inundación de paquetes de datos. Cuando un atacante origina dicho ataque, éste encuentra un camino hacia la victima. Cuando la victima se da cuenta que está siendo atacado, él puede cortar la ruta, originando un mensaje RRER dirigido al atacante. Los nodos intermedios por los que pasa el RRER borraran la ruta del atacante hacia la victima. El mensaje RERR podría quitar algunas rutas, las cuales, no están relacionadas con el ataque, estas rutas pueden ser reparadas por los nodos en el futuro. Así las rutas se van cortando y el ataque es gradualmente terminado. Cuando el ataque es terminado, el atacante puede originar un nuevo RREQ, y el nodo victima puede rehusarse a responderlo, no contestando con el RREP.

Pero ya que en el protocolo AODV los nodos intermedios pueden responder los RREQ si tienen rutas válidas aunque la victima no quiera que la ruta se reactive. Para evitar esto, la función de que los nodos intermedios puedan contestar RREQ debe ser cancelada. Solamente el destino puede responder los RREQ.

Conclusiones:

Se ha descrito el ataque por inundación, un ataque poderoso contra los protocolos de ruteo bajo-demanda para redes ad hoc. Este ataque permite al intruso montar un ataque de rechazo de servicio contra todos los protocolos de ruteo que trabajan bajo-demanda para redes móviles ad hoc, incluso los protocolos seguros. Se ha diseñado el protocolo llamado "Prevención del Ataque de Inundación" (FAP) para resistir el ataque. El FAP está compuesto de dos técnicas, qué son la supresión de vecino y corte de ruta, y éstas técnicas son capaces de defender el Ataque Inundando eficazmente.

Referencias:

Protocolo AODV:

http://www.faqs.org/rfcs/rfc3561.html

Protocolo seguro:

http://ieeexplore.ieee.org/iel5/9755/30769/01425219.pdf?tp=&arnumber=1425219&isnumber=30769