Resistencia a ataques de inundación en redes Ad Hoc

Flooding Attack Prevention

(FAP)

Temas a Tratar

- Introducción
- Ataque de inundación de RREQ
- Protocolo para evitar el ataque de inundación de RREQ
- Comparación entre ataques de inundación en redes Ad Hoc y redes alambricas
- Ataque de inundación de paquetes de datos
- Protocolo para evitar el ataque de inundación de paquetes de datos

Introducción

- Las redes son particularmente vulnerables a ataques de negación de servicio lanzado por un intruso
- El ataque por inundación en redes Ad Hoc es usado contra protocolos de ruteo bajo demanda (AODV, DSR)
- El intruso transmite masivamente paquetes Route Request o manda muchos paquetes de datos para terminar con el ancho de banda de las comunicaciones y recursos en los nodos y así la comunicación valida no puede ser llevada a cabo.

Introducción (cont.)

- En redes alambricas existe un ataque de inundación también, llamado SYN. Aquí el atacante manda muchas peticiones de conexiones TCP con una dirección falsa a una maquina victima. Cada petición causa… una vez que los recursos del nodo victima se han terminado, ninguna conexión TCP puede ser establecida, negando el servicio a legitimas peticiones.
- Cabe destacar que en este tipo de ataques el objetivo es consumir los recursos de toda la red y no atacar a un solo nodo como en el caso de SYN

Ataque de inundación de RREQ

- La inundación de paquetes RREQ en toda la red consumirá muchos recursos. Para reducir la congestión en la red, el protocolo AODV adopta los siguientes métodos:
  - Un nodo no puede originar más de RREQ_RATELIMIT mensajes por segundo
  - Después de tx un RREQ, el nodo espera el RREP
- Al primer tiempo el nodo fuente transmite un RREQ, el cual, espera un “round-trip time” para la recepción de un RREP.

Analizando AODV

- Si no se recibe dicho RREP, el nodo fuente manda un nuevo RREQ. El tiempo que esperará por el RREP en el segundo intento será de 2*round-trip time.
- Los paquetes son inundados primero en un área pequeña, definido por TTL (time-to-live) en las cabeceras IP. Si no se ha recibido el RREP, el área de inundación es alargado incrementando el TTL en un valor fijo.
- El procedimiento es repetido hasta que un RREP sea recibido por el nodo que origino el RREQ.

El ataque

- El atacante selecciona varias direcciones IP que no estén en la red, esto es, si el atacante conoce el alcance de las direcciones IP en la red, pero si no las conociera, el atacante selecciona de forma aleatoria una dirección IP. Esto lo hace ya que ningún nodo podrá contestar con un RREP para dichos RREQ.

El ataque (cont.)

- El atacante sucesivamente origina RREQ para estas direcciones IP vacías, sin considerar el RREQ_RATELIMIT por segundo y sin esperar por el RREP o por el tiempo round-trip.
- El valor TTL (time-to-live) del RREQ es puesto al máximo, esto es sin utilizar el método de expansión de anillo.
- En estos ataques, toda la red será inundada por paquetes RREQ del atacante.

Ejemplo

- H → intruso. Los nodos ya no pueden construir rutas entre ellos

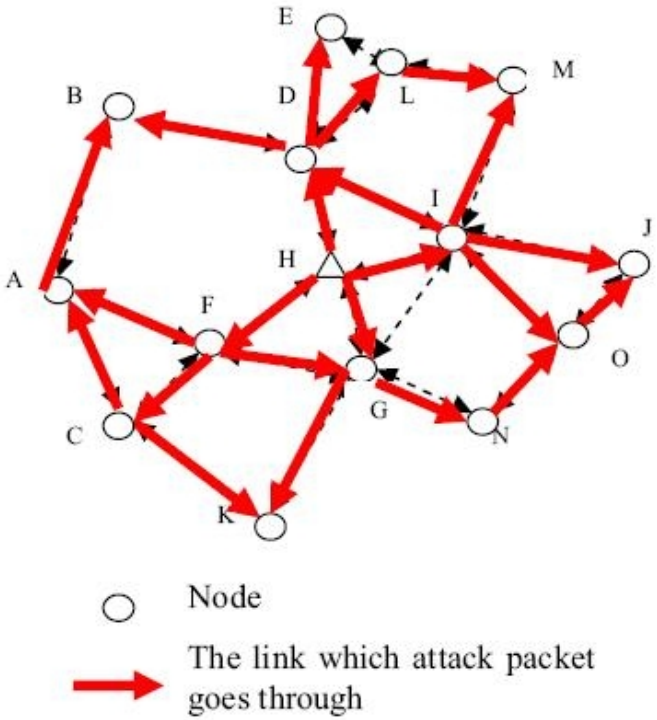
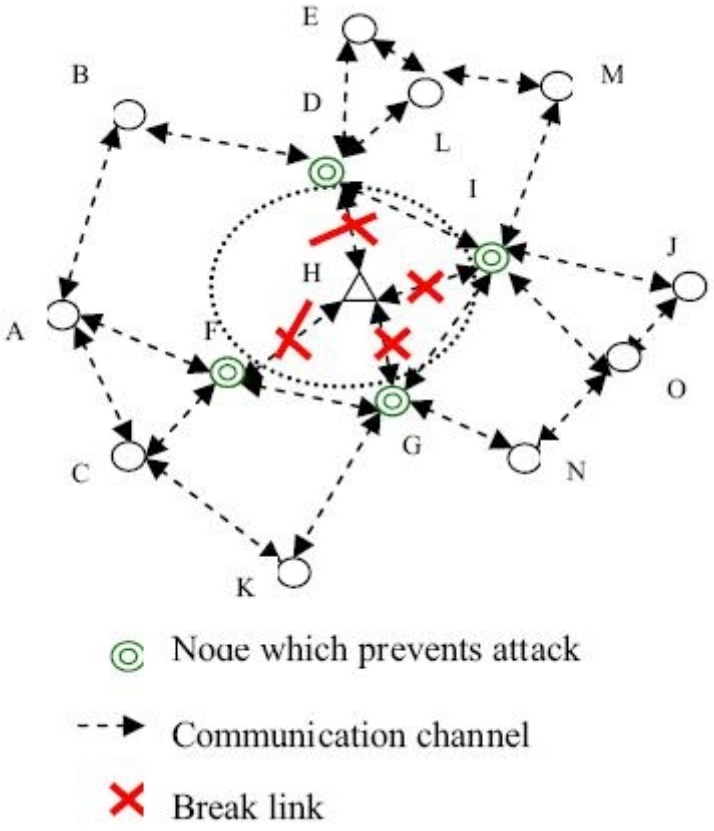


Figure1. The RREQ Flooding Attack

Solución: eliminación de vecinos

- Idea:
  - 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.

Los nodos vecinos aíslan al atacante



Descripción

- 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
- y 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.

Ejemplo

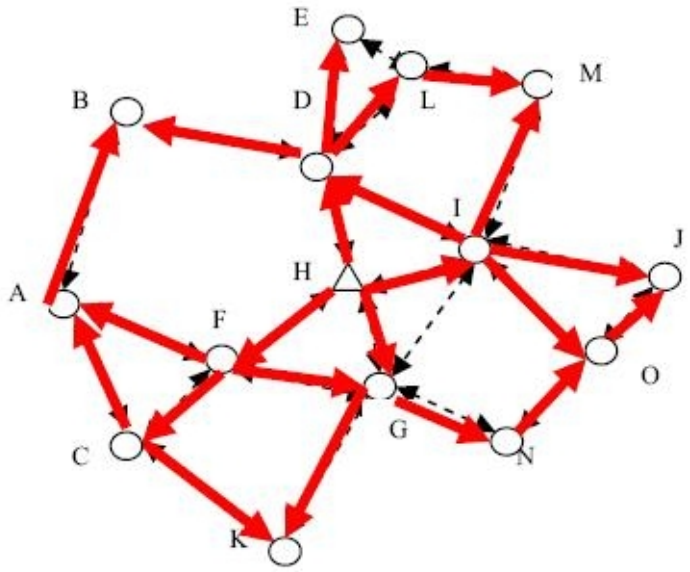


Figure1. The RREQ Flooding Attack

- Nodo F, los valores iniciales para prioridades en sus vecinos es de 1. A manda 2 RREQ, C manda 5 RREQ. Prioridad A→1/2 y C→ 1/5. Después los dos mandan un RREQ, A tiene mayor prioridad

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 tipicamente de 75 segundos.

Comparación (cont.)

- 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”.

Diferencias entre ataques de inundación de redes Ad Hoc y SYN

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

Ataque por inundación de paquetes 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.

Solución: corte de ruta

- Idea:
  - 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.

Descripción

- El atacante encuentra una ruta hacia el nodo victima.
- Cuando la victima se da cuenta que dichos paquetes de datos son inútiles, entonces él origina 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 estan relacionadas con el atacante, éstas rutas pueden ser reparadas por los nodos en el futuro.

Descripción (cont.)

- 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.

Descripción (cont.)

- 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.