CAPITULO 3

Objetivos de la tesis sobre DDOS

En este tercer capítulo y una vez ubicado el contexto actual o estado del arte sobre los ataques DDOS, realizaremos una breve descripción de los objetivos iniciales que nos plantearemos en nuestra tesis.

Obviamente estos objetivos son simples indicaciones que nos permitirán enmarcar nuestro trabajo dentro del ambiente de investigación existente. También servirán como punto de partida y nos permitirán marcarnos unas metas para la aportación a al comunidad científica.

3.1 Objetivos

El objetivo principal de nuestra tesis será el de **proporcionar una solución práctica y eficiente que permita minimizar el impacto de los ataques** de denegación de servicio distribuido.

De esta forma nos planteamos como una premisa inicial la imposibilidad real de evitar totalmente este tipo de ataques. En la coyuntura actual, tanto tecnológica como socialmente, los siguientes aspectos influyen determinantemente en la inviabilidad de una solución total:

1. Internet es una red heterogénea que se extiende por todo el mundo. La cantidad de países y gobiernos implicados imposibilitan la posibilidad de una legislación común.

2. La gran variedad de sistemas existentes tanto en software como en hardware conectados a Internet imposibilita el despliegue eficaz de cualquier tipo de medida universal.

3. Resulta del todo imposible la administración eficiente de todos los nodos conectados a Internet. El aumento diario de puntos de conexión y las tecnologías sin cable (*wireless*) hacen extremadamente difícil controlar las conexiones existentes en todo momento.

4. La posibilidad de falsear las direcciones IP o los ataques de tipo "*reflection*" imposibilita cualquier tipo de identificación del origen real del ataque. De esta forma no podemos tomar contra-medidas para aislar los focos reales de ataque.

De la bibliografía existente y de los trabajos realizados hasta el momento podemos concluir una serie de seis premisas que si bien no proporcionan la solución buscada si nos permitirán acotar el conjunto de soluciones posibles [Gib02][MP03][MP03-1][MP03-2] [Tan3][Ver03][Wat4][WWW19]…

I. Debemos utilizar una solución distribuida para atacar un problema distribuido.

II. La solución propuesta no debe penalizar el tráfico de los usuarios legítimos.

III. Debe ser común a todos los nodos de Internet y permitir su implantación con un coste razonable de recursos.

IV. También deberá ser incremental permitiendo su aplicación gradual manteniendo la compatibilidad con el resto de los sistemas dónde aún no haya sido implementada.

V. Debe integrar desde su diseño mecanismos de seguridad para la autentificación de los mensajes y mecanismos de cifrado para mantener la confidencialidad.

VI. Proporcionará adaptabilidad y proactividad ante el tráfico existente en cada momento.

3.2 Clasificación de los ataques DDOS

Podemos realizar decenas de clasificaciones para agrupar los distintos ataques DDOS existentes en la actualidad. Sin embargo, si profundizamos en su estudio vemos dos características fundamentales que comparten todos los ataques DOS/DDOS:

1. La finalidad principal de todo ataque de denegación de servicio simple o distribuido es conseguir el cese temporal de la actividad proporcionada por el objetivo.

   Todo y que se pueda alcanzar mediante el uso de distintas técnicas [Ver03] (ataques SYN Flood / IP Flood, Smurf, DRDOS…) en la práctica siempre acaba mostrando un consumo total de todo el ancho de banda que dispone el nodo atacado.

Las mínimas medidas de seguridad ante ataques DOS/DDOS actualmente consisten por un lado en ampliar la capacidad de la pila IP para poder absorber mas peticiones de conexión, y por otro en añadir mas servidores para que las conexiones se distribuyan de forma balanceada y no colapsen al servidor.

2. Los ataques DOS/DDOS que se registran pueden realizarse de forma directa (dónde el datagrama utilizado en el ataque ha sido creado en la dirección de origen), indirecta (dónde la dirección de origen ha sido falseada directamente o mediante técnicas de reflexión) o híbrida.

De esta forma podemos clasificar los ataques de denegación de servicio, y por tanto sus soluciones, en dos grupos (ver figura 3-1):

A. **Ataques directos**. Son aquellos en que los datagramas o peticiones recibidas por el objetivo del ataque provienen realmente de la dirección de origen especificada.

   Estos ataques son realizados desde ordenadores satélite o esclavos (*slaves*) dónde un atacante ha conseguido acceso de forma ilegal, ya sea infectándolo mediante un virus/troyano (MyDoom por ejemplo) o mediante un *exploit* o *root kit*, y los utiliza como plataforma de ataque remota.

B. **Ataques indirectos**. En este grupo ubicaremos los distintos ataques que falsean la dirección de origen con el objetivo de esconder su ubicación real y minimizar las posibles contra-medidas adoptadas por el objetivo del ataque.

   En este grupo también podemos incluir los híbridos o mixtos ya que presentan direcciones de origen falsificadas en mayor o menor grado.

   Contrariamente a lo que las estadísticas de ataques DOS/DDOS muestran, para este tipo de ataques **si que existe una solución** en la actualidad que permite su desactivación de forma efectiva, rápida y sin un coste adicional de recursos.

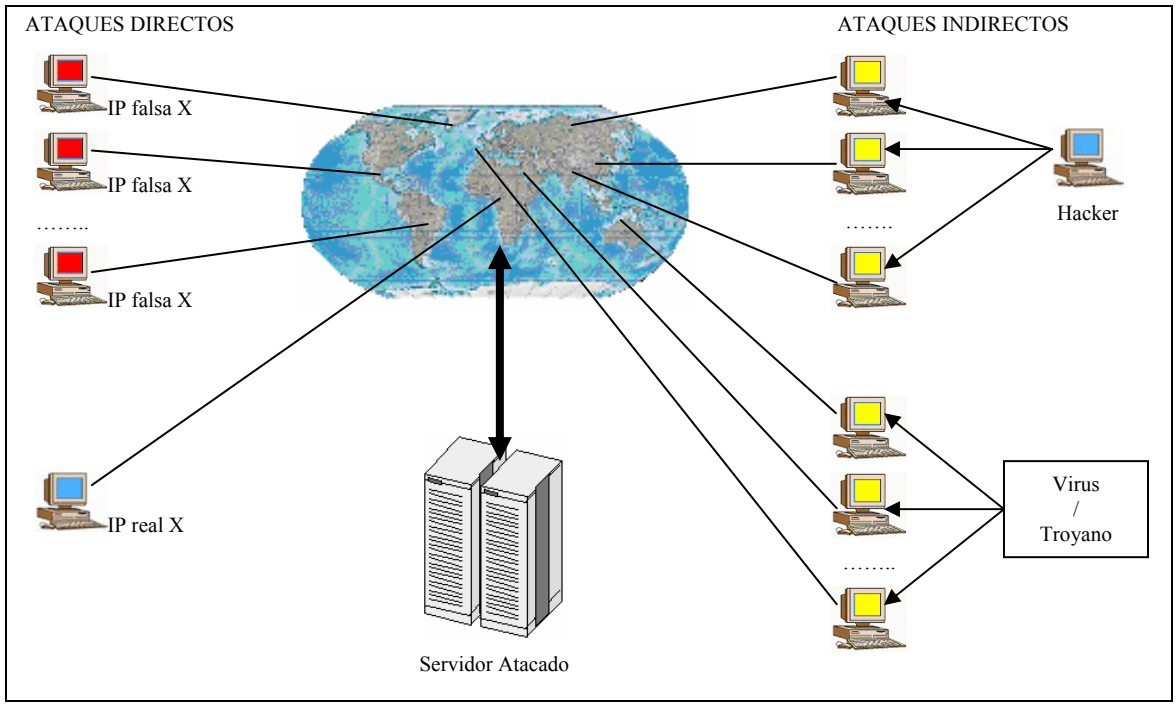

FIG 3-1: Ataques DOS/DDOS Directos e Indirectos.

3.2.1 Egress filtering

El filtrado de tráfico de salida o "*egress filtering*" [Hoe00][BK02][Sch03][UVS+03] [WWW47] tiene por objetivo el control de las direcciones IP utilizadas en la red dónde esté aplicado.

La idea subyacente consiste en que nosotros conocemos a priori el rango de direcciones IP válidas en nuestra red. De esta forma podemos poner un filtro que compruebe todo el tráfico de salida y elimine todos aquellos paquetes que no pertenezcan al rango de IP válido (ver figura 3-2).

El uso de este simple tipo de filtrado de red por parte de ISP, universidades y grandes organizaciones conectadas a Internet eliminaría todos los ataques de denegación de servicio indirectos. Desgraciadamente la permisividad o incompetencia de los administradores lleva a que no sólo millones de conexiones particulares carezcan de este filtrado, sino que los mismos proveedores o ISP muchas veces no lo implementan.

La Universidad Autónoma de Barcelona dispone de la clase B 158.109.0.0 / 255.255.0.0. De esta forma, en todo su tráfico de salida debería filtrar cualquier paquete IP que no contenga esta dirección IP de

En un router CISCO esto se transforma en:

```
access-list 150 permit ip 158.109.0.0 0.0.0.255 any
access-list 150 deny ip any any log

ip access-group 150 out                    ; Es importante que sea solo al tráfico de salida, ya que
                                             sino NO permitirá la entrada de ningún paquete!
```

FIG 3-2: Ejemplo de filtro de salida (egress filtering) en la UAB.

Si bien el filtrado de salida no puede evitar que en la red interna o local un ordenador falsee su dirección IP, si que evita el uso de nuestras redes (en caso de ser comprometidas por un atacante o virus) como trampolín de ataques DOS/DDOS a terceros.

3.2.2 Ingress filtering

El filtrado de tráfico de entrada o "*ingress filtering*" [CB94][WWW47][RFC2267] tiene como objetivo asegurar que todos los datagramas que entran a nuestra red provienen de direcciones IP rutables/reales o existentes.

El protocolo IP [RFC791] define su direccionamiento como un conjunto de 32 bits subdivididos en conjuntos o clases (ver figura 3-3). Cada una de estas clases presenta un rango reservado, también denominado en la bibliografía privado o no rutable, que se destina a redes IP que no se encuentran directamente conectadas a Internet.

El objetivo de estos rangos reservados es el de permitir su reutilización en todo tipo de redes privadas de forma que no fuera necesario utilizar direcciones únicas para redes que no debían estar conectadas a Internet.

CLASE	RANGO			DIRECCIÓN PRIVADA
A	0.0.0.0	Hasta	127.255.255.255	127.0.0.0
B	128.0.0.0	Hasta	191.255.255.255	172.16.0.0
C	192.0.0.0	Hasta	223.255.255.255	192.168.0.0
D	224.0.0.0	Hasta	239.255.255.255	N/A
E	240.0.0.0	Hasta	247.255.255.255	N/A

FIG. 3-3: Clases de direcciones IP en Internet.

En los ataques de DOS/DDOS indirectos las direcciones de origen se falsean de forma que no sea posible la detección de las auténticas fuentes del ataque. Una posibilidad básica consiste en utilizar como dirección de origen falsa la dirección de cualquier nodo conectado a Internet. En este caso el ordenador atacado responderá a las peticiones de conexión o de cualquier tipo a la dirección especificada por el atacante.

La otra posibilidad consiste en de utilizar como dirección falsa de origen la de los rangos privados (usualmente 127.0.01) de forma que el nodo atacado simplemente genere tráfico local hacia él mismo.

De esta forma el filtrado de entrada simplemente consiste en la comprobación de que ninguna dirección de origen en nuestro tráfico de entrada hace referencia a rangos privados no rutables.

Al igual que con el filtrado de salida, esta práctica no requiere de recursos suplementarios para su instalación y debería de ser de obligado cumplimiento en todos los organismos, universidades e ISP.

3.2.3 Conclusiones

La combinación del uso de prácticas de filtrado de entrada y salida (*ingress/outgress filtering*) nos permite reducir la posibilidad de un ataque DOS/DDOS indirecto.

No obstante en el caso de ataques de denegación de servicio distribuido directos, dónde la dirección de origen del datagrama es la dirección real del ordenador, este tipo de filtros no proporcionan ningún tipo de reducción o minimización de su impacto.

Tras estas conclusiones se ha demostrado que el problema real de los ataques DOS/DDOS es el uso de ataques directos. En este tipo de ataques dónde los orígenes de la denegación de servicio están realmente identificados no podemos actualmente realizar ningún tipo de contra-medida que no sea local.

De esta forma el ataque sigue consumiendo todo el ancho de banda que pueda entre los orígenes y el objetivo sin que pueda ser evitado o mitigado. Precisamente en dar respuesta a este problema basaremos el estudio de nuestra tesis.

3.3 Sistema de bloqueo de ataques DOS/DDOS

Nuestra tesis versará sobre el desarrollo de sistemas de bloqueo ante ataques DOS/DDOS. A continuación esbozaremos básicamente las ideas que se desarrollarán durante el doctorado.

Partiendo del punto final de nuestros estudios anteriores, nos encontramos con la siguiente situación (ver figura 3-4):

- Los ataques DOS/DDOS indirectos, aquellos en que se falsea la dirección de origen, pueden solventarse mediante la aplicación de técnicas de filtrado de entrada y salida.

- Los ataques directos siguen siendo inevitables debido a la imposibilidad de distinguirlos del tráfico normal de la red.

- La única forma efectiva y eficiente de parar este tipo de ataques es en su origen, ya que cualquier otra solución al final de la cadena permite el consumo de ancho de banda degradando el servicio a todos los usuarios.

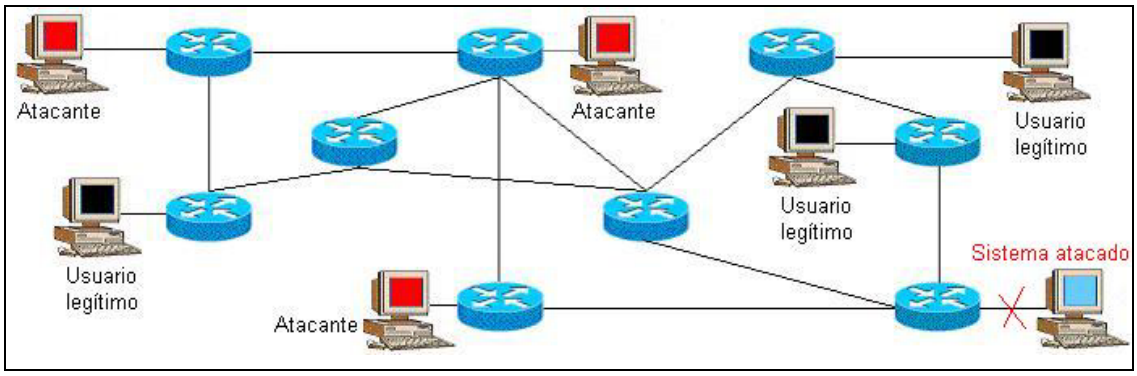

FIG. 3-4: Escenario de un ataque DDOS directo en Internet.

Actualmente la detección de ataques DOS/DDOS está bastante consolidada debido principalmente a gran crecimiento experimentado por los sistemas de detección de intrusos o IDS. En nuestro escenario de trabajo nos encontramos entonces con que ya por un lado ya conocemos el tipo de ataques de denegación de servicio distribuido que podemos encontrarnos y por el otro existen mecanismos de detección de este tipo de ataques.

Una vez analizado todo lo expuesto anteriormente queda únicamente dar propuestas de solución a un ataque DOS/DDOS ya detectado.

Destacamos nuestra intención expresa de no entrar en los mecanismos de detección de este tipo de ataques. Los sistemas IDS/IPS [Ver03] existentes en la actualidad ya son suficientemente maduros como para asumir su correcto funcionamiento. Por otro lado la complejidad y amplitud del estudio de la detección de ataques DOS/DDOS podría dar para otro doctorado.

3.3.1 Comunicación LAN objetivo - router

Este apartado se centrará en los pasos a seguir desde que nuestros sistemas locales detectan un ataque DOS/DDOS hasta que inician la respuesta.

Nuestro escenario actual es una red local dónde podemos encontrar diferentes máquinas que proporcionan servicios a los usuarios de Internet. También disponemos de un sistema de detección de ataques de denegación de servicio distribuido, ya sea un sistema detector de intrusos, un firewall o cualquier otro software o hardware que pueda realizar esta función (ver figura 3-5).

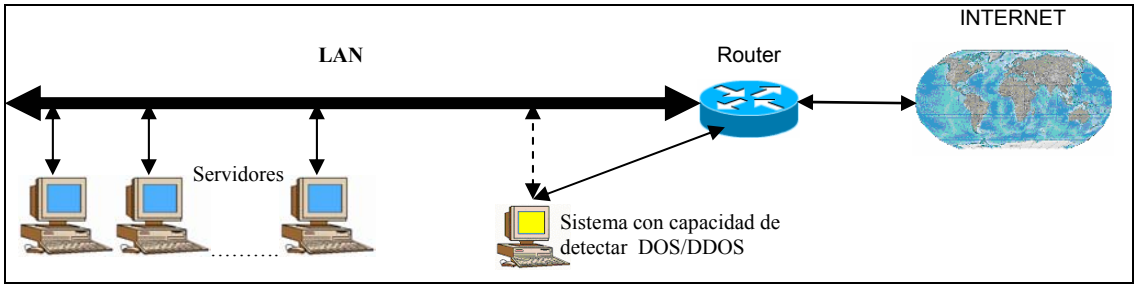

FIG. 3-5: Escenario de detección de un ataque DDOS.

En este esquema podemos observar como de forma "pasiva" el sistema de detección de ataques[ℜ] DOS/DDOS examina todo el tráfico de red hasta que decide que existe un ataque de denegación de servicio por parte de una o varias direcciones IP identificadas.

Puntualizamos que las técnicas de detección de ataques de denegación de servicio quedan fuera de este estudio y pueden ser implementadas a gusto del administrador de red. Técnicas heurísticas, reglas fijas de detección de conexiones por segundo…

Queremos hacer notar que el sistema de detección únicamente se encuentra conectado activamente al router de salida, con lo que evitamos su detección y posibles ataques tanto locales como foráneos.

[ℜ] Este sistema puede estar integrado con otros servicios como firewall, IDS….

Debido a que este sistema de detección es el desencadenante de la respuesta al ataque DOS/DDOS su seguridad e integridad deben estar garantizadas con un esquema como el propuesto anteriormente.

Una vez detectado el ataque DOS/DDOS por el sistema debe proceder a comunicar las direcciones IP y las máscaras correspondientes al router. El objetivo de comunicar la máscara correspondiente a la dirección IP en lugar de tratarla como 255.255.255.255 es el de proporcionar un sistema que permita bloquear rangos enteros.

Rara vez en un ataque distribuido se reciben peticiones de una sola máquina perteneciente a una red. Usualmente (como en el caso de los virus) el atacante se propaga por toda la red local del ordenador infectado.

Una vez que el router recibe del sistema detector DOS/DDOS las direcciones IP implicadas en el ataque, procede a bloquear su acceso durante 255 segundos y comunica una alerta administrativa a cada uno de los routers de salida a los que esté conectado con el objetivo de que realicen el mismo proceso.

La elección de un tiempo de 255 segundo (4 minutos y 15 segundos) obedece al tiempo máximo de vida de un datagrama IP [Ric98-1]. No debemos olvidar que nuestro objetivo es minimizar los efectos del ataque DOS/DDOS. Si se produjera un bloqueo permanente se podría privar de servicio a usuarios legítimos una vez desactivado el ataque.

En el probable caso de tener cientos o miles de direcciones IP envueltas en un ataque de denegación de servicio distribuido, se mantendrían sólo las 255 direcciones IP con su máscara de red correspondiente que más actividad registrasen. Por este motivo el análisis que realiza el sistema detector de ataques DOS/DDOS es fundamental y se ha extraído fuera del propio router.

Hemos de destacar también que al utilizar máscaras de red junto con la dirección IP nos permite en el peor caso poder bloquear 255 direcciones IP y en el mejor caso 255 rangos IP completos (ver figura 3-6).

CLASE	RANGO			MÁQUINAS
A	0.0.0.0	Hasta	127.255.255.255	2^24 16.777.216
B	128.0.0.0	Hasta	191.254.255.255	2^16 65.536
C	192.0.0.0	Hasta	223.254.254.255	2^8 256
D	224.0.0.0	Hasta	239.255.255.255	N/A
E	240.0.0.0	Hasta	247.255.255.255	N/A

FIG. 3-6: direcciones IP según su máscara de red.

La elección de 255 direcciones IP obedece por un lado a la simplificación que permitiría el uso de una look-up table ordenada por los últimos 8 bits de la dirección IP. Por otro lado que carece de sentido establecer más de 255 reglas de limitación de tráfico. Más reglas significa más comprobaciones del router y por tanto una penalización en su rendimiento.

La discusión de la seguridad, autenticación y confidencialidad de las comunicaciones entre el sistema detector de ataques de denegación de servicio y el router se introducen en el capítulo 3.3.4.

3.3.2 Comunicación router - router

Este apartado trata sobre cómo se realiza la propagación de la alerta administrativa generada por el router de la red local atacada.

Las alertas administrativas siempre se comunicarán entre sistemas adyacentes (ver figura 3-7). De esta forma un router sólo puede enviar mensajes a los routers que tiene físicamente conectados a sus interfaces.

Este sistema se realiza principalmente para evitar sobrecargas (*overhead*) de comunicaciones entre routers distantes varios grados. Si estamos sufriendo un ataque de denegación de servicio el ancho de banda disponible es mínimo, con lo que las comunicaciones a routers alejados pueden resultar imposibles.

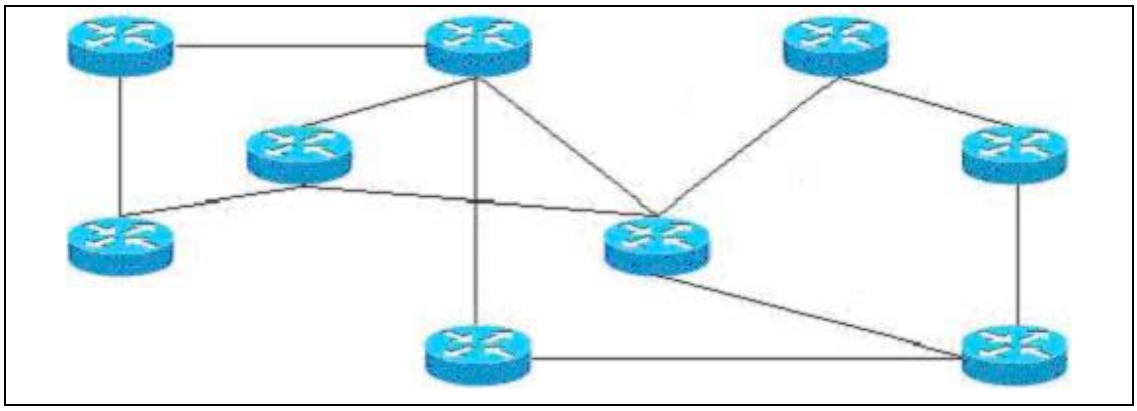

FIG. 3-7: Propagación de mensajes entre routers adyacentes.

Por otro lado este sistema elimina los problemas de seguridad en la autenticidad y privacidad de las comunicaciones recibidas ya que al ser conexiones punto a punto un posible atacante externo tiene más difícil el introducir tráfico espurio.

La comunicación entre routers se podrían realizar en cualquiera de las cuatro capas que nos proporciona el modelo OSI [Ric98-1][Ver03] (ver figura 3-8):

- **Paquetes TCP:** Permitiría el establecimiento de conexión y un intercambio de datos fiables añadiendo una cierta sobrecarga (*overhead*) en las transmisiones.

  La comunicación a este nivel permitiría el desarrollo de aplicaciones y protocolos más complejos sustentados en la fiabilidad que proporciona.

- **Datagramas UDP:** Paquetes básicos sin conexión ni fiabilidad que llevarían el campo de tiempo de vida (TTL) igual a 1. De esta forma cualquier intento de ataque externo tendría pocas posibilidades de prosperar.

- **Frames MAC:** En este nivel la conectividad no se realizaría a través de la familia de protocolos TCP/IP, sino que aprovechando la comunicación entre routers adyacentes se intercambiarían frames directamente.

  Cabe destacar que este tipo de comunicación depende directamente del medio físico utilizado, y que por tanto no es común a todas las tecnologías.

APLICACIONES (Applications)	WWW, SSH, FTP...
TRANSPORTE (Transport)	TCP, UDP, ICMP...
RED o Interconexión de redes (Network)	IP
ENLACE o Red real (Link)	IEEE 802.2, 802.3...

FIG. 3-8: Estructura de cuatro capas.

Una vez que un router recibe una alerta administrativa legítima comprueba si recibe paquetes IP desde la dirección solicitada. Si es así continúa la propagación de la alerta a todos los routers adyacentes excepto al router del que la recibió.

El propio router conoce en un tiempo finito y determinado si recibe paquetes desde la dirección IP solicitada ya que estamos bajo un ataque DOS/DDOS. Si no los recibe desestima la alerta y continúa su trabajo de forma normal.

En el caso de recibir una alerta que ya ha incluido en su tabla de direcciones a bloquear también la deshecha y no la propaga. De esta forma eliminamos la posibilidad de bucles infinitos y tráfico redundante. Si a los 255 segundos (tiempo máximo de perduración de una regla) recibe otra alerta volvería a colocar la dirección IP en la tabla de sistemas bloqueados.

La discusión de la seguridad, autenticación y confidencialidad de las comunicaciones entre routers se introducen en el capítulo 3.3.4.

3.3.3 Comunicación router – LAN origen

Conforme el proceso de propagación de las alertas administrativas contra ataques de denegación de servicio vaya circulando hacia el origen (u orígenes) del ataque, llegará un momento en que alcanzará el router conectado a la red local dónde reside el atacante.

Una vez alcanzado este punto el router debería bloquear el acceso hacia fuera de las direcciones IP implicadas en el ataque y enviar una alerta administrativa a los administradores de la red.

El caso ideal consistiría en la posibilidad de avisar directamente al ordenador objeto del ataque que desistiera de acceder de forma temporal a la dirección IP atacada. No obstante este grado de eficiencia implicaría la existencia de un servicio en cada ordenador que pudiera proceder en este sentido.

Una de las premisas enunciadas en nuestro trabajo hacía referencia a la necesidad de que el despliegue de esta solución fuera gradual. En nuestro caso hemos descrito el flujo completo desde la detección del ataque DOS/DDOS hasta la propagación de la alerta administrativa al ordenador responsable del ataque.

En el caso real de que no todos los routers intermedios implementen a la vez esta solución, conseguiríamos como mínimo nuestra primera intención de minimizar el impacto del ataque. Tal y como se ha comentado un ataque de denegación de servicio se basa en el consumo de todo el ancho de banda disponible, los routers que implementen este sistema eliminarán el ataque en su medida liberando ancho de banda tanto para el sistema atacado como para el resto de usuarios de Internet.

Esta propuesta mejora las soluciones aportadas actualmente basadas en costosos y complejos sistemas y algoritmos que únicamente permiten la eliminación de los ataques en la red final.

3.3.4 Mecanismos de comunicación segura

Los distintos mecanismos de comunicación que se proponen en esta solución van encaminados a proporcionar desde su diseño la autenticidad y privacidad de los mensajes intercambiados entre los distintos sistemas.

La familia de protocolos TCP/IP fue diseñada para el intercambio de información entre dos sistemas cualesquiera conectados a Internet. De esta forma por su construcción no ofrecen mecanismos de autenticación de direcciones IP de origen y destino ni confidencialidad de los datos intercambiados.

En nuestra solución propondremos diferentes esquemas que proporcionaran las cotas de autenticidad y privacidad que la comunidad juzgue necesaria. El uso de técnicas de intercambio de claves y mecanismos de cifrado que se propone es el siguiente [RH91] [Rif95][Sch96] [MOV01][FS03]:

- **Modo de trabajo simple**: En este paradigma se definiría una comunicación basada únicamente en el intercambio de datagramas UDP. De esta forma no habría establecimientos de conexión ni fiabilidad en la entrega de los datos.

  Cuando un router decidiera enviar una alerta administrativa construiría un datagrama UDP que enviaría a los routers adyacentes con la información necesaria sobre la dirección IP y la máscara de red a bloquear. En este caso se indicaría en el campo de tiempo de vida (TTL) el valor 1 para evitar bucles o ataques de terceros.

  La sobrecarga (*overhead)* existente en este modelo es mínima, ya que permite una comunicación ágil sin necesidad de establecimiento de conexión.

  Este modelo permitiría añadir características de autenticación y cifrado mediante la pre-negociación entre pares adyacentes de una clave privada y el uso de algoritmos criptográficos como DES, IDEA…

- **Modo de trabajo fiable seguro**: En este modo se utilizaría un intercambio de mensajes seguros mediante el protocolo TCP. De esta manera tendríamos que el router mantendría una comunicación "abierta" con cada uno de los routers adyacentes para el intercambio de mensajes.

Este modelo es actualmente utilizado por algoritmos de rutado en Internet como el BGP y permitiría mantener la fiabilidad entre los distintos interfaces de los routers en momentos de stress ya que el propio protocolo TCP implementa la retransmisión de mensajes.

La ampliación de este modo de trabajo de forma que garantice las cualidades de autenticidad y cifrado es similar al anterior. Sin embargo esta fiabilidad en las comunicaciones permitiría la extensión a modelos de clave pública (RSA, Diffie-Hellman…) sin limitarse a los routers adyacentes.