Tendencias en Ciber-Seguridad: Ataques de Denegación de Servicio

IMPLANTACIÓN CORPORATIVA DE TECNOLOGÍAS, SERVICIOS Y SISTEMAS INFORMÁTICOS

Máster en Ingeniería Informática

Ignacio Gago Padreny

Facultad de Informática

Universidad Complutense de Madrid

Madrid, Junio de 2016

Índice General

Capítulo 1

Objetivos de este trabajo

El campo de la ciberseguridad informática ha tomado especial interés en los últimos años, convirtiéndose en una fuente de estudio para muchos investigadores. El objetivo de este trabajo es el estudio de los ataques de denegación de servicio, tanto sus métodos como sus defensas, debido a la gran relevancia que tienen estos dentro del campo de la ciberseguridad.

Capítulo 2

Introducción

Los ataques de denegación de servicio constituyen una de las amenazas más importantes y extendidas en el ámbito de la ciberseguridad, según datos de [1] aumentando un 125 % año tras año. Además de crecer en frecuencia, también crece en sofisticación y en ancho de banda. En cuanto a la sofisticación están aprovechando últimamente vulnerabilidades en servidores DNS y en el protocolo NTP (Network Time Protocol), usado para sincronizar fechas y horas entre distintas máquinas de una red. En cuanto al ancho de banda estos ataques han aumentado en volumen, con ataques sostenidos de 200 Gbps[2]. Sin embargo, muchas empresas no están preparadas para este tipo de ataques e incluso muchas de ellas desconocen esta amenaza (un 40 % de las empresas no está preparada para este tipo de ataques[2]). Estos ataques además tienen muchas veces por objetivo el encubrimiento de delitos como pueden ser transferencias fraudulentas de dinero o el desanonimato[4].

Los ataques de denegación de servicio (del inglés *Denial of Service Attacks*) o DoS, tienen como objetivo comprometer la disponibilidad de un servicio agotando sus recursos. Estos ataques pueden intensificarse en ancho de banda al originarse desde diversas máquinas en lugar de solamente una, conociéndose entonces como ataques de denegación de servicio distribuidos (DDoS). Estos ataques distribuidos suelen realizarse utilizando botnets (una red de ordenadores comprometida). Básicamente estos ataques se llevan a cabo mediante dos métodos distintos: mediante inundación que consiste en agotar los recursos mediante un número muy alto de peticiones haciendo que usuarios legítimos no puedan ser atentidos (por ejemplo el ataque ICMP) y mediante vulnerabilidades que consiste en aprovechar fallos (de implementación normalmente) de algún protocolo (por ejemplo la conocida vulnerabilidad *Heartbleed* de la librería OpenSSL)[3].

El crecimiento de los ataques de denegación de servicio es debido a diversos factores, que se suelen clasificar en función de las motivaciones del mismo. Algunas de ellas son[3]:

- **Económicas:** se basan en reducir el poder de la competencia al inutilizar los recursos. Suele ser bastante frecuente en empresas de videojuegos multijugador online, en los que empresas competidoras tratan de inutilizar los servidores de la otra empresa para ganar consumidores.

- **Creencias:** grupos políticos o culturales que expresan su contrariedad frente a otro tipo de creencias.

- **Experimentación:** individuos que tratan de mejorar sus habilidades cometiendo este tipo de ataques, para posteriormente utilizarlos con otro tipo de motivaciones.

El crecimiento y la variedad de estos ataques hacen que sea difícil desarrollar una estrategia defensiva que prevenga estos ataques debido a la gran diversidad de formas que hay para realizarlos. A pesar de esta variedad muchos utilizan técnicas comunes que son la inundación, la amplificación y la reflexión.

DoS basada en inundación Esta es la forma más burda pero también más simple de realizar un ataque de denegación de servicio, se basa en la inyección de grandes volúmenes de tráfico. Estos ataques actúan sobre la capa de red o sobre la capa de aplicación. En el caso de la capa de red los protocolos más explotados son TCP, UDP, ICMP y DNS[5]. Un ejemplo es la inundación SYN del protocolo TCP que se aprovecha del *Handshake* para abrir conexiones falsas en un servidor y que este se quede sin recursos para abrir más conexiones. En el caso de la capa de aplicación el protocolo HTTP es el más explotado.

DoS basado en reflexión La reflexión se basa en intentar ocultar el origen del atacante falsificando la dirección IP origen (IP spoofing). De esta forma se utiliza por ejemplo en el ataque *smurf* provocando que todas las máquinas respondan a la dirección IP origen falsa, en este caso la víctima no sería la dirección IP destino, sería la dirección IP origen. También existen ataques de este tipo sobre VoIP[7].

DoS basado en amplificación La amplificación se basa en utilizar terceras partes que generen un paquete de mayor tamaño, de esta forma, falsificando también la dirección de retorno (también utilizan la reflexión) la victíma recibe paquetes de

gran tamaño originados con un ancho de banda menor. El ejemplo más común de este tipo de ataques se basa en el protocolo DNS, cuyas respuestas pueden tener un tamaño muy grande comparado con el de la consulta[8].

Capítulo 3

Botnets

En este capítulo se tratarán las botnets, uno de los medios más habituales que utilizan los atacantes para realizar ataques de denegación de servicio distribuidos, que además de aumentar el ancho de banda del ataque hace inútil el proceso de identificación del origen.

El término botnet designa a un conjunto de máquinas infectadas (conocidas como bots), que están bajo control de un operador humano (conocido como el botmaster). Los bots son utilizados para llevar a cabo gran variedad de acciones maliciosas y dañinas contra sistemas y servicios, incluyendo ataques de denegación de servicio, distribución de spam y phishing. Están diseñadas con motivos económicos y normalmente el botmaster pone en alquiler la botnet en servicio de terceros a cambio de remuneraciones económicas[30].

La arquitectura de una botnet como se ha mencionada anteriormente, está compuesta por bots (que viene de robot, pues siguen las instrucciones que les da un operador humano) y por el botmaster, que se comunica con ellos mediante mensajes C&C (Command and Control), por lo que se deben establecer canales para dicha comunicación, que usualmente están basados en IRC. Normalmente estos bots se adquieren por el botmaster mediante la infección de los equipos utilizando vulnerabilidades que permiten el acceso con superusuario al ordenador comprometido, haciendo que el dueño del equipo infectado sea un participante pasivo de los actos delictivos[30].

3.1. Ejemplos de botnets

En esta sección se presentan algunas de las botnets más importantes descubiertas hasta la fecha. A pesar de que se comente principalmente su función en cuanto al envío de spam por email hay que tener en cuenta que los ataques de denegación de

servicio que han podido causar no han sido detectados o no se conseguido identificar su origen, por lo que no hay que deshechar que realizarán esta actividad. Estas botnets y otras vienen comentadas en [31].

- **Grum** fue creada en el año 2008, y en cuatro años se convirtió en responsable de hasta el 26 % de todo el spam de Internet por email. En el año 2010 era capaz de emitir hasta 39.9 billones de mensajes por día, convirtiéndola en la botnet más grande descubierta hasta esa fecha.

- **ZeroAccess** es una de las botnets más recientes en ser detectada y cerrada. Se estimaba que tenía el control sobre 1.9 millones de ordenadores distribuidos por todo el mundo y su provecho económico se basada en *click fraud* y minería de bitcoins. Fue descubierta por la minería de bitcoins, pues consumía energía suficiente para dar luz a 111000 casas cada día.

- **Windigo** se descubrió en el año 2014 y su nombre viene de un mitológico monstruo caníbal. Habiendo operado durante solamente tres años, había infectado 10000 servidores Linux (no ordenadores), permitiendo enviar 35 millones de emails con spam cada día. Curiosamente, mandaba distinto contenido en función del sistema operativo del dispositivo que lo iba a recibir: enviaba malware a Windows, páginas web de citas a usuarios de Mac OS X, y contenido pornográfico a usuarios de iPhone.

- **Cutwail** controlaba dos millones de ordenadores en el año 2009, mandando hasta 74 billones de emails con spam cada día (más o menos 1 millón por minuto). En ese momento era el 46.5 % del spam mundial total.

- **Srizbi** solamente estuvo activo durante un año, a pesar de ser responsales del 60 % del spam mundial de 2007 a 2008. Cuando se desarticuló está botnet, el spam mundial cayó un 75 %.

Capítulo 4

Ataques de Denegación de Servicio

En este capítulo se van a exponer una serie de ejemplos ilustrativos de ataques de denegación de servicio clasificados en función del nivel de capa TCP/IP. Además, se comentarán unos ataques que han tenido gran relevancia dentro de la ciberseguridad por su magnitud.

4.1. Nivel de red

Se aprovecha de vulnerabilidades en protocolos a nivel de red, como pueden ser TCP, UDP, ICMP y DNS.

4.1.1. Inundación SYN

El protocolo TCP utiliza una establecimiento de conexión consistente en el *Handshake*:

1. El cliente envía un paquete SYN al servidor.
2. El servidor responde con SYN ACK y almacenará la información requerida en memoria.
3. El cliente confirma su petición enviando un paquete ACK.
4. El servidor comprueba en su pila de memoria si se encuentra tal conexión.
5. En caso de encontrarse la transferencia puede empezar.

Durante las inundaciones SYN el atacante envía al servidor muchos paquetes SYN con direcciones falsas o inexistentes de forma que el servidor almacenará toda esta información, sin embargo no confirmará ninguna conexión con un paquete ACK.

De esta forma el servidor quedará bloqueado con conexiones semiestablecidas que nunca llegarán a establecerse, impidiendo el acceso a usuarios legítimos[32].

4.1.2. Inundación NTP

Recientemente han aparecido este tipo de ataques (a partir del año 2013) y suelen realizarse a páginas web de juegos y proveedores de servicios de Internet (ISP). La razón es que al igual que DNS, se basa en el protocolo UDP y se puede conseguir una respuesta de gran tamaño con una pequeña consulta. NTP es el protocolo usado por máquinas conectadas a Internet para ajustar sus relojes y es usado por equipos de escritorio, servidores y también teléfonos móviles. Desafortunadamente, este simple protocolo basado en UDP es dado a la amplificación (y reflexión) pues responderá a un paquete con un dirección IP origen falsificada y porque al menos uno de sus comandos enviará una respuesta grande a una solicitud pequeña, lo que le convierte en un medio para los ataques de denegación de servicio. NTP contiene un comando conocido como *monlist* (a veces MON_GETLIST) que se envía a un servidor NTP con propósito de monitorización, el servidor enviará hasta 600 direcciones IP de las últimas máquinas que han interactuado con el servidor. El paquete de solicitud es de 234 bytes, mientras que las respuestas en el caso de haber 600 máquinas son de 48000 bytes, produciéndose un factor de amplificación de 206. Afortunadamente hay mejoras que permiten agregar seguridad a este protocolo, pero no todos los servidores las implementan[34].

4.2. Nivel de aplicación

Ante el uso masivo de páginas web a diario en todas partes del mundo, el protocolo HTTP es uno de los protocolos más propicios para camuflar un ataque y pasar desapercibido. Por esto es uno de los protocolos en los que más se buscan vulnerabilidades.

4.2.1. Ataques de inundación de sesión

La idea es iniciar muchas sesiones HTTP con un servidor y no permitir la conexión de los usuarios legítimos. Este ataque se distingue fácilmente al tener un *session rate* muy elevado[33].

4.2.2. Ataques de inundación de peticiones

En este caso la idea se basa en realizar más peticiones que las que es capaz de atender el servidor. El ataque GET/POST *flooding* (inundación) envía muchos request/post desde una botnet, saturando el servidor con peticiones que resolver. Una versión de este ataque es el single-session GET/POST flooding, que aprovecha que a partir de HTTP 1.1 pueden realizarse varias peticiones por sesión, lo que implica un session rate más bajo y evadir posibles mecanismos de defensa[33].

4.2.3. Ataques Request/Response lenta

Una forma de saturar el servidor y evitar que usuarios legítimos accedan a él es mantener todos los sockets disponibles por el servidor ocupados. Normalmente un servidor HTTP cierra una conexión en cuanto satisface la petición que recibe. Este tipo de ataques se caracterizan por ser más inteligentes e intentar mantener la conexión HTTP abierta el máximo tiempo posible y agotar el número de sockets disponibles.

Slowloris[33]

Slowloris se basa en enviar peticiones muy lentamente, para esto envía peticiones HTTP parciales, sin rellenar la cabecera (no envía el salto de línea que separa la cabecera y el cuerpo), de forma que el servidor se queda esperando los datos que finalicen la petición. El atacante enviará una cabecera ampliada intentando apurar al máximo los timers de finalización de sesión para mantener la conexión abierta el mayor tiempo posible.

Fragmentación HTTP[33]

La idea es la misma que en el caso de Slowloris, pero en este ataque se fragmentan paquetes legítimos en múltiples partes y todas estas se envían lentamente. Al ser paquetes legítimos este ataque suele realizarse desde botnets.

Slowpost/RUDY[33]

El ataque Slowpost o RUDY (R-U-Dead-Yet?) utiliza comandos *post* en los que ha definido previamente en la cabecera del paquete HTTP la longitud que enviará en el cuerpo del paquete. Una vez se ha hecho esto, envía el cuerpo del mensaje con una tasa de 1B cada dos minutos.

Slowreading[33]

El ataque Slowreading, como su nombre indica, se basa en leer las respuestas del servidor lentamente. Para esto se aprovecha del protocolo TCP y al establecerse la conexión anuncia un tamaño de ventana menor que el buffer de envío del servidor. De esta forma el protocolo TCP se mantiene alerta de un posible cambio de tamaño de ventana para el cual tiene asociados unos timers. Aunque no exista comunicación HTTP, TCP mantendrá abierta la conexión en base a esos timers esperando poder enviar los datos.

4.3. Hitos en la historia de los ataques de denegación de servicio

- El 7 de Febrero del año 2000 un estudiante de 14 años (apodado MafiaBoy[24]) consiguió realizar con éxito ataques de denegación de servicio a Yahoo!, Fifa.com, Amazon.com, Dell, Inc., E*TRADE, eBay y CNN. Solamente lás pérdidas en Yahoo! se contabilizaron como 1.2 billones de dolares americanos.
- El 18 de Marzo del año 2013 Spamhaus recibió un ataque de denegación de servicio de 10Gbps, que delegó en la empresa CloudFare. CloudFare pasó a recibir las peticiones dirigadas a Spamhaus y dejo el ataque para aprender de él pues no comprometía su red. Los atacantes dedicideron aumentar la fuerza del ataque llegando hasta los 300Gbps, siendo hasta el momento el ataque con más ancho de banda recibido hasta la fecha (que se tenga constancia)[28].
- El 15 de Enero de 2015 más de 19000 páginas web francesas fueron atacadas como consecuencia de lo sucedido en la revista Charlie Hebdo[29].
- En el 2016 Anonymous atacó los servidores DNS raíz turcos con 40Gbps[26].
- En Enero de 2016 un ataque dejó durante tres horas la página web de la BBC y las del candidato Donald Trump con picos de hasta 602Gbps[27].

Capítulo 5

Estrategias defensivas

Los ataques de denegación de servicio suponen un gran reto para la ciberseguridad puesto que es muy difícil desarrollar un sistema defensivo contra estos. Normalmente los sistemas se clasifican según el momento del ataque en el que actúan: prevención, detección, identificación del origen y mitigación. Todas estas fases son importantes y los sistemas más sofisticados deben tratar cada una de las fases para ser lo más completos posibles. Cada una de estos cuatro ejes han sido tratados con profundidad en la bibliografía y tratan de adaptarse a los nuevos ataques que surgen.

5.1. Prevención

Los métodos pertenecientes a este grupo actúan antes de que el propio ataque suceda y tratan de por una parte minimizar el daño a recibir en caso de que ocurra un ataque y por otra parte disminuir la probabilidad de que ocurra un ataque. A pesar de ser una parte importante de los sistemas de defensa son insuficientes sin las demás partes. En [6] se enumeran algunas de los métodos usados en esta fase.

5.2. Detección

Sin duda la fase más importante de cualquiera de los sistemas defensivos puesto que sin esta fase no habría cabida para la identificación del origen ni para la mitigación. Sin embargo es posiblemente la fase más difícil. Su eficacia se basa en la proporción de ataques reales que son detectados, aunque también deben tener en cuenta los falsos positivos, pues es importante no emitir alertas a menudo ante situaciones legítimas de tráfico. Los falsos positivos además acarrean una dificultad añadida debido al fenómeno conocido como *flash-crowd*, que sucede cuando se produce una acumulación inesperada de accesos a un servidor pero de forma legítima,

como fue el caso del mundial del 98[9].

En cuanto a la detección hay dos paradigmas claramente diferenciados: reconocimiento de firmas y detección de anomalías. El reconocimiento de firmas se basa en mantener una historia de la mayor cantidad de ataques reales conocidos y realizados y comparar el tráfico entrante con esta base de datos en busca de similitudes. Sin embargo la identificación de patrones en el reconocimiento de firmas tiene la gran desventaja de que pequeñas variaciones de ataques ya existentes tendrán patrones distintos y no serán detectados lo que hace que sea una herramienta poco efectiva en un área donde continuamente evolucionan los ataques y aparecen nuevos. Por otra parte la detección de anomalías se basan en modelar el comportamiento habitual del tráfico de la red e identificar eventos anómalos que difieran de las características del tráfico legítimo. Este método sí que puede detectar nuevos ataques o variaciones de ataques ya existentes pero es más difícil de llevar a cabo un sistema basado en anomalías que uno basado en reconocimiento de firmas. En la actualidad el método que más predomina es la detección de anomalías con gran variedad de técnicas distintas: modelos basados en Markov[10], teoría del caos[12], algoritmos genéticos[11], análisis CUSUM[13], lógica difusa[14] o el estudio de las variaciones de la entropía aplicando modelos estadísticos[15][16].

Muchas de las técnicas que más se utilizan en cuanto a la detección de anomalías es el uso de la entropía[22][23], pues la entropía es un indicativo de lo homogéneo/heterogéneo que es un conjunto de datos. En la mayoría de los ataques de denegación de servicio (por lo menos los de inundación) el tráfico atacante tiene unas características muy similares por lo que al haber gran cantidad de este tipo de paquetes se tiene un tráfico muy homogéneo, mientras que en condiciones de tráfico legítimo el tráfico suele ser más heterogéneo. La entropía se aplica como una métrica que permitirá modelar el sistema de diversas formas, algunas de ellas series temporales (como el caso de Holt-Winters o ARIMA), en las que en función del pasado se predecirá el próximo valor de la entropía con un umbral de error, cuando este umbral es traspasado se emitirá una alerta pues se ha detectado una anomalía.

5.3. Identificación del origen

En esta etapa, que sucede siempre después de haber detectado el ataque, la víctima trata de encontrar la ruta del vector de ataque para descubrir al atacante. Este proceso es muchas veces complicado puesto que el atacante dispone de variados métodos para ocultar su rastro que van desde sencillos procesos de suplantación de

identidad hasta incluso hacer uso de redes anónimas. A pesar de no poder encontrar la ubicación real del atacante, acercarse lo máximo posible permite una defensa más efectiva[17].

En [18] se presentan distintos métodos y sus diferencias para la identificación del origen, muchos de ellos basados en el marcado de la ruta de los paquetes, ya sea marcando el propio datagrama o almacenando información en dispositivos intermedios.

5.4. Mitigación

La mitigación trata de mitigar el daño causado y sus medidas consisten usualmente en el incremento de recursos de sistema o el aumento de la restricción en sistemas de autenticación.

Capítulo 6

Métodos de evaluación

Uno de los problemas en el área de los ataques de denegación de servicio son los pocos datos públicos y abiertos que existen sobre ataques realizados, incluyendo las trazas. Por esto es muy difícil para la comunidad científica valorar y estimar las estrategias defensivas. Como se explica en [35], la mayor parte de las colecciones públicas de muestras de ataques carecen de validez por diferentes motivos, ya sea por antigüedad o falta de rigor en los procesos de captura. A continuación se van a mencionar y comentar las dos colecciones más usadas:

- **KDD'99.** Estas muestras están recogidas del concurso KDDcup del año 1999 e incluye parte de un conjunto de trazas de ataques publicadas por la agencia norteamericana DARPA. Además de ser un dataset antigüo, no solamente incluye tráfico de denegación de servicio sino que también incluye otro tipo de ataques lo que le hace perder validez científica. Los datos presentes en las muestras han sido totalmente anonimizados y no se tienen las trazas originales, sino que se tienen expresadas en función de 41 parámetros.

- **CAIDA'07.** Contiene trazas de ataques de inundación como ICMP, SYN y HTTTP en formato reconocible por Wireshark, capturadas en el 2007[20]. Es el dataset que los científicos consideran más válido a pesar de que tiene el problema de que solamente contiene tráfico de ataque y por lo tanto no puede establecerse un modelo del tráfico legítimo para detectar una anomalía posteriormente. Para realizar el modelo se suele usar la colección CAIDA'08[21] que contiene tráfico legítimo del mismo router aunque un tiempo después.

Capítulo 7

Valoración personal

En los últimos años la ciberseguridad ha sido una de las ramas más estudiadas en informática, con el gran problema que supone que siempre las defensas se han desarrollado ante los ataques existentes lo que ha suponido que las defensas estaban muy retrasadas con respecto a los ataques. Entre la diversidad de ataques que existen uno de los que ha tenido gran relevancia son los ataques de denegación de servicio, que causan pérdidas económicas muy grandes a las empresas afectadas. A pesar de los avances en cuanto a la defensa y detección de los ataques se refiere, los atacantes buscan nuevas formas más sofisticadas para burlar estas defensas. En mi opinión, debe trabajarse en la modelización del tráfico legítimo de las redes para poder llevar a cabo una detección de anomalías precisa y con un número muy bajo de falsos positivos. Para ello no solamente se debe trabajar en las defensas sino que se deben desarrollar de forma controlada ataques y generar datasets con muestras y dar un marco de valoración efectivo a los investigadores para poder medir la calidad de los sistemas defensivos. Además, las causas principales de que existan los ataques de denegación de servicio son la posibilidad de falsificar la dirección IP origen y la existencia de botnets. Trabajar en implementar en todos los dispositivos de Internet el protocolo seguro IPsec podría dar solución al primero de los problemas, y mejorar la seguridad de cada uno de los equipos que se conectan a Internet también debe ser una prioridad para reducir el riesgo de infección de equipos para conformar botnets. A pesar de estar mencionando varios problemas abiertos y complicados que existen ahora mismo para solucionar este problema, es importante ver que hay muchos desafíos aún que resolver y que la mejora de cada uno sirve para resolver muchos otros problemas existentes.

Bibliografía

[1] Akamai (2016)."Q1 2016 State of the Internet". Available: https://www.akamai.com/uk/en/about/news/press/2016-press/akamai-releases-first-quarter-2016-state-of-the-internet-security-report.jsp

[2] SANS Institute (2014). "DDoS Attacks Advancing and Enduring: A SANS Survey". Available: https://www.sans.org/reading-room/whitepapers/analyst/ddos-attacks-advancing-enduring-survey-34700

[3] T. Peng, C. Leckie, K. Ramamohanarao. "Survey of network-based defense mechanisms countering the DoS and DDoS problems", *ACM Computing Surveys*, Vol. 39 (1), no. 3, pp. 1-42, 2007.

[4] R. Jansen, F. Tschorsch, A. Johnson, B. Scheuermann, "The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network", *in Proc. of the 18th Symposium on Network and Distributed System Security (NDSS)*, San Diego, Ca, US, August 2014.

[5] C. Douligeris, A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", *Computer Networks*, Vol. 44 (5), pp. 643–666, April 2004.

[6] S. T. Zargar, J. Joshi, D. Tipper. "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *IEEE Communications Surveys & Tutorials*, Vol. 15 (4), pp. 2046-2069, March 2013.

[7] H. Sengar, H. Wang, D. Wijesekera, S. Jajodia. "Detecting VoIP Floods Using the Hellinger Distance", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19 (6), pp. 794-805, June 2008.

[8] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, S. Gritzalis. "DNS amplification attack revisited", *Computers & Security*, Vol. 39, part B, pp. 475-485, November 2013.

[9] W. Zhou, W. Jia, S. Wen, Y. Xiang, W. Zhou. "Detection and defense of application-layer DDoS attacks in backbone web traffic", *Future Generation Computer Systems*, vol. 38, pp. 36-46, January 2014.

[10] S. Shin, S. Lee, H. Kim, S. Kim. "Advanced probabilistic approach for network intrusion forecasting and detection", *Expert Systems with Applications*, Vol. 40, no. 1, pp. 315-322, 2013.

[11] S.M. Lee, D.S. Kim, J.H. Lee, J.S. Park. "Detection of DDoS attacks using optimized traffic matrix", *Computers & Mathematics with Applications*, Vol. 63, no. 2, pp. 501-510, September 2012.

[12] Y. Chen, X. Ma, X. Wu. "DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory", *IEEE Communications Letters*, Vol. 17, no. 5, pp. 1052-1054, May 2013.

[13] C. Callegari, S. Giordano, M. Pagano, T. Pepe. "Wave-cusum: improving cusum performance in network anomaly detection by means of wavelet analysis", *Computers & Security*, Vol. 31, no. 5, pp. 727-7J5, July 2012.

[14] P.A.R. Kumar, S. Selvakumar. "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems", *Computer Communications*, Vol. 36, no. 3, pp. 303-19, February 2013.

[15] I. Ozcelik, R.R. Brooks. "Deceiving entropy based DoS detection", *Computers & Security*, Vol. 48, no. 1, pp. 234-245, February 2015.

[16] M.H. Bhuyan, D. K. Bhattacharyya, J.K. Kalita. "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection", *Pattern Recognition Letters*, Vol. 51, no. 1, pp. 1-7, January 2015.

[17] A.R. Kiremire, M.R. Brust, V.V. Phoha. "Using network motifs to investigate the influence of network topology on PPM-based IP traceback schemes", *Computer Networks*, Vol. 72 (1), pp. 14-32, October 2014.

[18] N.M. Alenezi, M.J. Reed. "Uniform DoS traceback", *Computers & Security*, Vol. 45 (1), pp. 17-26, September 2014.

[19] S. Khanna, S.S. Venkatesh, O. Fatemieh, F. Khan, C.A. Gunter. "Adaptive selective verification: an efficient adaptive countermeasure to thwart DoS attacks", *IEEE/ACM Transactions on Netwowking*, Vol. 20 (3), pp. 715–728, June 2012.

[20] The CAIDA UCSD (2015), "DDoS Attack 2007 Dataset". Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml

[21] The CAIDA UCSD (2015), "Anonymized Internet Traces 2008". Available: http://www.caida.org/data/passive/passive_2008_dataset.xml

[22] C.E. Shannon. "A mathematical theory of communication", *Bell system technical journal*, Vol. 27, pp.397-423, 1948.

[23] A. Rènyi. "On measures of entropy and information", *in Proc. of the 4th Berkeley symposium on mathematical statistics and probability*, Berkeley, CA, US, Vol. 1, 547-561, June 1961.

[24] MafiaBoy. https://en.wikipedia.org/wiki/MafiaBoy

[25] PCMag (2014). Available: http://www.pcmag.com/article2/0,2817,2453157,00.asp

[26] Radware (2016). Available: https://blog.radware.com/security/2016/01/top-ddos-attacks-2015/

[27] TheHackerNews (2016). Available: http://thehackernews.com/2016/01/biggest-ddos-attack.html

[28] Cloudfare (2013). Available: https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/

[29] The Whir (2015). Available: http://www.thewhir.com/web-hosting-news/thousands-french-websites-face-ddos-attacks-since-charlie-hebdo-massacre

[30] Rafael A. Rodríguez Gómez, Gabriel Maciá Fernández, Pedro García Teodoro. "Survey and Taxonomy of Botnet Research through Life-Cycle", 2013.

[31] We Live Security (2015). Available: http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/

[32] Wikipedia. Available: https://en.wikipedia.org/wiki/SYN_flood

[33] Saman Taghavi Zargar, James Joshi, David Tipper. "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, *IEEE Communications Surveys & Tutorials*, Vol. 15 No. 4, Fourth Quarter 2013.

[34] Cloudfare (2014). "Understanding and mitigating NTP-based DDoS attacks". Available: https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

[35] S. Bhatia, D. Schmidt, G. Mohay, A. Tickle. "A framework for generating realistic traffic for Distributed Denial of Service attacks and Flash Events", *Computers & Security*, Vol. 40, no. 1, pp. 95-107, February 2014.