Methodologies for detecting DoS/DDoS attacks against network servers

Mohammed Alenezi
School of Computer Science & Electronic Engineering
University of Essex name
Colchester, UK
mnmale@essex.ac.uk

Martin J Reed
School of Computer Science & Electronic Engineering
University of Essex name
Colchester, UK
mnmale@essex.ac.uk

***Abstract*—As denial of service (DoS) attacks are becoming more common in the Internet, there is greater need for solutions to overcome these attacks. Defending against DoS/ DDoS attacks can generally be divided into 3 phases: prevention, detection and response. Detection is one of the key steps in defending against DoS/ DDoS attacks. However, with the high variation in the DoS/DDoS attack types, the detection of such attacks becomes problematic. A good detection technique should have short detection time and low false positive rate. This paper presents an introduction to intrusion detection systems (IDS) and survey of different DoS/DDoS detection techniques. The key observation of this survey paper is that a CUSUM-based detection technique has many advantages over other statistical instruments in that it is non-parametric; consequently, it does not require training and is more robust to variations in the attack profile.**

Keywords-DoS; DDoS; detection; network security.

I. INTRODUCTION

As DoS attacks become one of the most threatening security issues, the need to detect this type of attack is increasing. DoS is not just a "game" played for fun by some attackers, it has become an effective weapon for cyber war or for so called "hacktivist" groups [1]. In general, detection is required before the spread of a DoS attack. DoS detection is often part of a wider intrusion detection system (IDS) [2, 3]. An IDS is best defined as software or hardware used to detect unauthorized traffic or activities that are against the allowed policy of a given network [4]. Intrusion detection is not a new research field, with one of the earliest published IDS papers in 1980 by Anderson [5]; in 1987, Denning [6] provided a structure for researchers working on IDS [2]. IDS can be classified based on the serving component (the audit source location) as either host-based, network-based or a combination of both. In a host-based IDS the audit information, such as application and operating system log files, are monitored while the network traffic is monitored in a network-based IDS. The host-based is usually located in a single host while the network-based system is usually located on machine separate from the hosts that it protects [7]. Hybrid intrusion detection systems combine both the network and host-based systems [8].

The rest of this paper is organized as follows. In section II, an overview of the IDS is presented, while in section III DoS detection is introduced. In section IV, general DoS classification is presented with different proposed techniques and discussion. The classification of DoS flooding-based attack is presented in section V. Our key observations about the detection techniques are presented in section VI.

II. IDS OVERVIEW

Network-based IDS (NIDS) usually detects attacks such as worms, scans, DoS attacks, botnets, and other types of attacks [9]. In the following, a general overview of the IDSs will be presented. Then, more precisely DoS detection techniques will be reviewed.

Network IDSs are generally categorized based on the detection method as one of two types: signature-based or anomaly-based detection. Signature-based, also known as rule- or misuse-based [10], detects an attack by comparing well-known attack signatures, or patterns, with the monitored traffic. A match generates an alarm for a potential attack. This type has fast detection time, detects most known attacks [11], and, generally has a low false positive rate, *i.e.*, it does not signal an alarm for legitimate traffic. On the other hand, an anomaly-based IDS, also known as behavior-based, operates by comparing the network traffic behavior against previous "normal" traffic behavior. Any deviation in the comparison is considered to be a sign of an attack. The system acquires a normal traffic profile, usually through training, and monitors the traffic for any differences with the normal profile [12]. The normal traffic behavior is classified into two types [11]: standard and trained. The standard is based on standard protocols and rules such as TCP handshaking connection [13] set up and how the attacker could perform a half connection attack. The trained traffic is used to determine a threshold value for future detection. There are many network anomaly-based systems and interested readers can refer to [11]. Anomaly detection can detect unknown attacks; however, it generally produces higher false positive rates than signature-based systems. Figure 1 summarizes the IDS classifications. In practice, systems may combine both signature and anomaly-based techniques.

In general, anomaly-based intrusion detection systems operate in three phases [14]: parameterization, training, and detection. In parameterization, the parameters of the system are defined. The model of the normal behavior of the traffic will be built in the training phase. In the detection phase, the traffic behavior is compared against that in the training phase. If the comparison exceeds a threshold value a detection alarm is triggered.

 ISBN: 978-1-61208-231-8

III. DoS Detection

A. Overview

DoS prevention using ingress filtering [15] can help in reducing some types of attacks such as spoofing IP addresses as used by attackers to hide their identity. However, reactive techniques are often required and here detection is needed to alert about the attack and perform some automatic action. A DoS/DDoS attack is considered to be just one type of attack that an IDS can react to and there are different types of network DoS including: overloading a service with seemingly legitimate requests and sending malformed packets, which aims to cause a failure of the service through some bug in the service. This paper considers the former rather than the latter type, as malformed packet-based DoS is relevant to general host-based security and can be filtered using a rule-based approach.

One of the key elements in DoS detection technique is the time of detection [16]. A good detection mechanism should detect the DoS attack before the service starts to be degraded. However, packets from an overloading type of DoS are often indistinguishable from those of legitimate users. This makes the detection difficult and increases the chance for a false positive, which is a critical problem in DoS detection. A good detection technique should react quickly and have a low false positive rate.

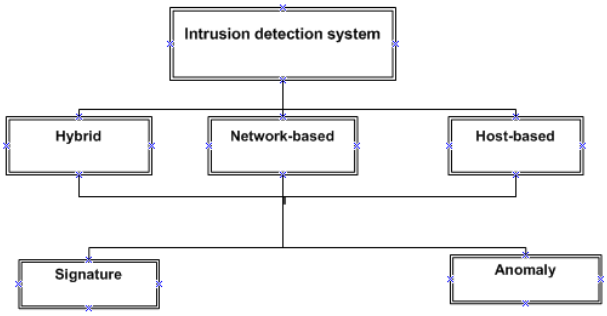

Figure 1. General classification of IDS

B. Classifications of DoS Detection

DoS detection techniques can be divided, as for general IDS, into signature and anomaly-based detection. Signature detection is based on well-known DoS attacks patterns [16], which are mostly malformed packets and protocol attacks. Anomaly detection is based on the traffic deviation from "normal" which is the form of most DoS attacks. The scope of this paper is anomaly-based DoS detection techniques for the overloading type of DoS [14]. However, even within this category, DoS detection techniques address different types of DoS attack such as a SYN flood attack[17] or a DNS attack [18, 19].

Different classifications have been proposed to provide a framework for the detection techniques. The differences are in the method used to detect the DoS attacks. Because of the paper length limitation, only three different proposed classifications were chosen. We have classified two works under general DoS detection classification and one under specific DoS flooding attack. A general description for each classification work will be presented, and some of the related techniques will be reviewed in the following sections.

IV. General DoS Classification

General DoS classification will cover two presented works. The first work was proposed by Peng [16]. The detection methods in this work were divided into: DoS attack specific detection and anomaly-based detection. DoS attack specific detection covers a general and wide range of different detection techniques types under one classification. In anomaly-based detection, the techniques are based on a comparison between the network traffic and a prepared normal traffic profile. The second work was proposed by Yonghua [17]. The detection techniques were divided into two types: IP attribute-based and traffic volume-based. The IP attribute-based technique monitors the behavior of selected IP attributes and considers the anomalies as deviations. The traffic volume-based studies the traffic of the network and applies statistical calculations on the packet rate of network flow.

A. Discussion

Peng [16] proposed two classifications for DoS detection techniques: DoS attack specific detection and anomaly-based detection. In DoS attack specific detection, the classification was made without regard to the methodologies in the detection; instead it was made to cover certain proposed techniques. For example, the authors have classified Multi Level Tree for Online Packet Statistics (MULTOPS) [20] and SYN detection techniques under the DoS specific detection. However, a closer inspection shows that it can be quite difficult to accurately classify such techniques. For example, the MULTOPS technique is quite different from the SYN detection technique, and it is not clear that the SYN is not, in fact anomaly-based detection.

Yonghua [17] proposed two classifications for DoS detection techniques: IP attribute-based and traffic volume-based. In IP attribute classification, certain parameters of the IP packets are monitored to detect the attack. For example, the source IP address, port number, or the time to live (TTL) value will be monitored as the values will show some change during an attack. In the IP attribute-based classification, the authors cover the techniques that deal with IP header parameters and emphasize the use of the TTL field. The traffic volume-based category covers any techniques that are not studying the IP header parameters. Many different methodologies placed in the traffic volume-based classification such MULTOPS, SYN detection, and other techniques that are based on statistical algorithms.

As mentioned earlier, signature-based detection is based on certain known characteristics in the traffic. Kompella [21] mentions that it is difficult to create a signature for a DoS attacks as the attackers could change the type and the content. Furthermore, Cheng [22] states that signature-based detection can be used to detect the communication between the attackers and their zombies. However, the communication could be encrypted making this detection

 ISBN: 978-1-61208-231-8

difficult. Consequently, Peng [16] states that signature-based detection is inefficient for DoS detection. However, we think signature-based should not be dismissed for the following reasons. First, although it is difficult to create signatures for all types of DoS, this fact applies to IDS more generally and not specifically DoS. There are certain types of DoS attacks that are straightforward to detect with a signature-based technique such as a TCP mixed flags attack. Second, Cheng [22] noted during the study one particular attack tool (Stacheldraht v1.666) that the communication between the attackers and the zombies can be detected using a signature-based approach. This is highly useful for the prevention stage. Consequently, while signature-based detection has limitation it can be highly effective in some cases.

The presented work by Peng [16] and Yonghua [17] provides a general classification for DoS detection techniques. Both of the works have different naming for the classifications and are overlapping in the mentioned techniques. In the following section, some of the proposed detection techniques will be reviewed.

B. Detection Techniques

A DDoS detection technique is proposed in [23], which is based on the source IP address. The system monitors the new source IP address of the packets instead of monitoring the traffic. The technique is based on the study by Jung [24], which indicates that during an attack, most of the source IP addresses are new. On the other hand, during flash crowds most of the IP addresses are not new. A flash crowd is a dramatic increase in the load on a web server by a, legitimate, large traffic surge causing an increase in congestion and packet loss [24]. The main drawback of this technique is that the attacker could launch a DoS attack by known (not new) IP addresses to the target to circumvent the detection system. The attacker can start normal communication with the target then perform the attack. Additionally, not all of the DoS attacks use spoofed IP addresses for example the attacker could use zombies with real IP addresses.

Talpade [25] proposes a detection technique based on the characterization of the dynamic statistical properties of the network traffic such as time to live (TTL) and other IP header information to detect the anomaly in the traffic. The characteristic of this idea is based on the change in the statistical distribution of the TTL values which indicates an anomalous change in the traffic. The main drawback is that the change in the TTL values does not always associate with anomalous traffic. Also, the model was not proposed for DDoS specifically.

Kim [26] proposes a detection technique based on creating a stable baseline profile to monitor the deviations in the traffic. An analysis was conducted to check the stability of the traffic with regards to different parameters. Significant differences in traffic patterns were found between different sites. Therefore, a baseline profile that is based on different attributes was proposed for detection. The choice of the attributes was based on the assumption that some of the attributes such packet size, TCP flag pattern, and protocol types can be anticipated by the attacker. On the other hand, based on the author's opinion, attributes such as TTL, source IP prefixes, and server port distribution are site dependent and difficult for the attacker to learn. Thus, the technique was proposed based on these attributes. The work presented in [26] has some drawbacks such as the chosen attributes are not directly related to DDoS attacks and there is added computational complexity with a high false positive rate [17].

Yonghua [17] proposed two DDoS detection techniques based on distance. Average distance estimation is the first one and the second is distance-based traffic separation. By analyzing the distance value and traffic rate, the attack can be detected. The TTL value is used to infer the distance value in the average distance estimation technique. The "normality" of the traffic is determined by the prediction of the mean value of the distance, where the prediction of the mean value was achieved by using the exponential smoothing estimation technique [27]. The second technique, distance-based traffic separation, uses the prediction of traffic arrival rates from different distances and thus the normality of the traffic is defined. The prediction of traffic arrival rates is achieved by using the minimum mean square error (MMSE) linear predictor technique. The normality and abnormality can be separated in the traffic for both techniques by using the mean absolute deviation (MAD).

Yonghua's techniques encountered the following drawbacks: first, the detection is based on the distance which is inferred from the TTL value. The distance will not reflect the real anomaly in the traffic. The attacker can know the distance to the victim and explicitly choose the path. Also, a sophisticated attacker can fix the TTL value to be within the predicted distance. Furthermore, the paths are subjected to change and different policies could be applied by different IPSs. Finally, for both of the techniques, the prediction of the normality of the traffic is achieved through the use of existing estimation techniques which are affected by the samples and can be anticipated by the attacker.

MULTOPS is proposed by Gil and Poletto [20]. It is a heuristic and data structure-based technique used by routers to detect a DDoS attack. The packet rate statistics for subnet prefixes are maintained by the nodes of the tree. The statistics are collected from different aggregate levels. The size of the tree is expandable with regards to the available memory. MULTOPS assumes the packet rate for the normal traffic in the communication between two machines is proportional. Therefore, any disproportional in the packet rate would trigger an alarm for the attack.

MULTOPS encounters some limitations mentioned by the authors. The location and set up of MULTOPS routers in the network would affect the ability of the technique to detect attacks with randomized IP source addresses packets. Legitimate packets for a certain IP destination address will be dropped as the MULTOPS would be confused by the spoofed IP address packets and identify the destination address to be under attacks. Furthermore, large number of attackers could connect to the victim in a normal way and the flows rate of the attackers' traffic is still proportional which means MULTOPS will not detect the attack. For example, large number of attackers could connect to the victim

 ISBN: 978-1-61208-231-8

through HTTP or FTP requesting a large file download. The victim will not be able to handle all of the requests consequently DoS and MULTOPS will not be able to detect the attack because the flow rate is proportional. Additionally, MULTOPS will suffer from a high false positive rate with streaming services as their flows are disproportional [16].

A detection technique for SYN flooding was proposed by Wang [28]. It is based on the normal behavior of TCP protocol (i.e. handshaking process and FIN or RST) and the sequential change point detection. The sequential change point detection is a statistical method to check for a change in a data [29]. To make the technique easy to use and more general, a non-parametric cumulative sum (CUSUM) method was used. The technique compares the ratio of SYN packets to the FIN or RST to find a change. One of the drawbacks of this technique that is the attacker could send the FIN or RST along with the SYN packet to avoid the detection [16].

A DoS detection technique was proposed by Blazek in [30]. The technique is based on statistical analysis on the data from different network layers to detect a change. The technique consists of two methods: adaptive sequential and batch sequential. The technique is based on the change point detection theory. To achieve a fixed rate of false alarms, statistical analysis of training data was utilized by both methods. The authors claim that their technique has three features: the methods are self-learning; the attacks can be detected with small delay; and computational complexity is manageable. The technique uses different traffic types such TCP and UDP in change detection modeling. The main drawback of the technique is the high computational complexity.

One of the key issues in DoS detection is how to discriminate between legitimate and attacker traffic to reduce the false positive rate. Cheng [31] proposes a technique, which is based on spectral analysis, to differentiate between normal traffic and attacker traffic. In order to use the spectral analysis in a packet-based network, a signal was defined as the number of arrival packets in a fixed length time interval. The power spectral density of the signal is estimated to discover the periodicity. Based on the fact that the periodicity around the round trip time of the normal TCP flows is strong in both directions while the attack flows are not, the attack is detected. The technique is not able to detect any attack other than TCP flows. Other protocols such UDP would pass undetected by the technique. A sophisticated attacker can send attack traffic at the same periodic interval to avoid detection such as low-DoS. The attack traffic does not have to be from a single source to form high volume. An attacker could use the zombies to send normal behavior traffic to the victim. However, the large number of zombies would be enough to overwhelm and deny the service from the victim [16]. Kulkarni [32] proposed a detection technique ,which is based on Kolmogorov complexity, to detect DDoS attacks. Kolmogorov complexity calculates the size of the smallest representation of the data and measures the degree of the randomness [33]. In general, it is based on the correlation between the traffic flows to distinguish between the attack traffic and high legitimate load traffic. It is been assumed that during the DDoS attack, the generated packets tend to have similar characteristics such as protocol type, destination address, type and execution pattern. All of the attack packets from different locations will have the same destination address which gives a similarity for the traffic pattern. This similarity can be detected by using the Kolmogorov complexity-based technique. On the other hand, the high load legitimate traffic tends to contain different types and characteristics which make the traffic flows to be randomly distributed and not greatly correlated. The technique is based on correlation and assumptions which are not always would be valid in case of the attack as the attackers can create a random flow to avoid the detection.

Cabrera [34] proposed a technique to proactively detect DDoS by using a time series analysis. The correlation between the traffic behavior at both of the victim and the attacker is the basis for this technique. A normal profile is built in order to compare any deviation in the traffic from the normal behavior to signal an attack alarm. In order to build the normal profile, key variables and correlation process need to be identified. Key variables are extracted at the victim side and then the variables, from the attackers, that are correlated to the extracted key variable are calculated by statistical tools such as Granger Causality Test (GCT) and Auto Regressive Model (AR Model) etc. For example, the key variable could be the ICMP echo packets at the victim and the variables correlation could be the ICMP replies [16]. To harden the detection process, different attack traffic could be combined in one type to make the correlation process is very complex as there will be many key variables to be correlated. It is been assumed that the same attack tool will be used from the sources of the attacks which is not always the case [16].

V. NETWORK BASED DOS FLOODING CLASSIFICATION

A survey for detecting DoS flooding-based attacks was presented by Carl [35]. The detection techniques are classified based on the algorithms used (not a certain parameter or behavior) into three groups: activity profiling, sequential change point detection, and wavelet analysis. Each group represents a general framework for the detection process.

A. Activity Profiling

Inside the header of the packet, certain information of the network traffic is monitored to generate an activity profile. The average packet rate for a network flow is defined as the activity profile. Consecutive packets with similar header fields such as protocol, port and addresses represent the network flow. The activity level or the average packet rate can be determined by the elapsed time between the consecutive matching packets. The average packet rates of all inbound and outbound flows are used to calculate the total network activity by dividing the sum over the average packet rates [35].

A high number of flows could be resulted by monitoring certain protocol services and this number will be increased for different services and protocols. Therefore, clustering concept was used to avoid the dimensional problems [35].

 ISBN: 978-1-61208-231-8

Individual flows with similar characteristics can be grouped in a cluster. The summation of constituent flows is used to determine the activity level of the cluster. The activity level of the clusters will be used to detect the attack based on an increase in the activity levels between the clusters which indicates an increase the attack rate. Distributed denial of service could cause an increase in the overall clusters.

The backscatter analysis project [36] is an example of the activity profiling. The authors were trying to estimate the worldwide DoS activity. During the attack, mostly the attacker uses packets with spoofed source IP addresses and when the victim replies to the spoofed source addresses, the packets will be backscattered. The backscattered packets are monitored and clustered based on the source address which is the victim's address. The normality of the distribution of the clustered backscattered packets, which is calculated by using Anderson-Darling test, is used to detect the attacks and define the threshold of the cluster's activity level.

Feintien [37] proposes an activity level DDoS detection technique. It is based on statistics and entropy of some of the IP header's attributes. For selected attributes such as IP source address, the entropy and Chi-square distribution are calculated for different cluster flows. Each cluster is categorized according to how frequent the source address of the packet has been seen. For example, the first cluster represents the most frequent source address seen in the traffic while the second holds the next 4 most seen source address. The third, fourth, and the fifth hold the next most 16, 256, and 4,096 source addresses respectively [35]. The last cluster will hold the rest of the traffic. Based on calculations, the DDoS can be detected by comparing the abnormal to normal traffic. The main drawback is the choice of the attribute that will be used for entropy calculation [17].

B. *Sequential Change Point Detection*

In sequential change point detection [35], the traffic is filtered at the victim, according to different criteria, such as address, port, and protocol. The filtered traffic is treated as a time series. For an attack starting at time $\mathcal{F}$, a change will be shown in the calculated statistics at time $\geq \mathcal{F}$. A Cumulative sum (CUSUM) [29] is one of the change point detection algorithms. It requires less computational and memory resources than other change point detection algorithms. CUSUM can be applied to DoS attacks by comparing the actual average for the traffic in the time series with the expected average. For a given time series sample, the difference between the actual and expected average is calculated. The CUSUM recursively will increase in case the difference exceeds an upper bound for attack traffic. On the other hand, the difference in the normal traffic will be under the bound and the CUSUM will be decreased. The DoS attack could be identified by defining a threshold that would specify the allowed increase in the time series within the upper bound. Based on the behavior of the network such as the expected volume of traffic or the range of delay that can be tolerated or the sensitivity of the running applications, CUSUM algorithms can trade-off between the detection delay and false positives rates during the setting of the threshold and the upper bound [35].

C. *Wavelet Analysis*

The input signal, in wavelet analysis, is described as spectral components in wavelets. With wavelets, the time for a given frequency can be determined as the wavelets provide a description for concurrent time and frequency. On the other hand, the Fourier analysis provides only a frequency description [35]. The time-localized anomalous signals can be separated from the noise signals by wavelets. By analyzing each spectral window's energy, the anomalies can be determined.

Paul *et al.* [38] proposed a detection technique based on wavelet analysis. The analysis was applied to four anomaly types: measurement failure, attacks, flash crowds, and outages such as network failures. The data used for the analysis was collected on a border router of a large university over six months. The data consists of IP flow and SNMP [39] measurements, which are decomposed into different time series. High and mid- band spectral energies are presented by applying wavelets on each time series.

VI. KEY OBSERVATIONS

As a result from reviewing the presented work on IDS and DDoS detection, key issues were observed which could help in studying DoS/DDoS detection. We believe that there are many aspects that should be considered towards getting a reliable detection system. It is not only depending on the technical details of the detection technique, other issues should be considered such as the following. First, the location of the machine that will carry on the detection process is vital and related to the design of the system. It could be a host-based where the traffic received and analyzed by the host or a network-based where the network traffic is monitored by a separate dedicated machine. Another choice is a hybrid system which combines both host and network types. Based on the protected system (protected system points to the system that installed the IDS), the location should be considered. For example, protecting a single server is different from protecting an ISP network that includes many hosts, servers and network resources. Second, considering the nature of the service provided by the protected system is part of the good design. Protecting a web server is different from protecting database server in terms of the information sensitivity, response time and the availability of server. Third, the choice for the used methodology such as anomaly-based or signature-based would make a difference. The choice should be based on the nature of the expected traffic and type of service provided by the protected system. For example, if the system is connected to the Internet or locally to private networks. There is a trade-off between anomaly-based and signature-based detection methodologies. Table I shows a comparison between the two methodologies. The same can be applied to DoS/DDoS detection. In DoS/DDoS, the detection is divided into two phases: the selected attributes to be monitored and the statistic methods. The selected attributes should show different behavior during the attack. The statistic methods would discover the abnormality in the selected attribute. Choosing adequate attributes would make significant difference in detection

 ISBN: 978-1-61208-231-8

time. Additionally, choosing the right statistic method among the wide available range would help in discovering the abnormality in the attribute very fast.

In the experience of the authors, the CUSUM statistical techniques perform better than other statistical techniques due to many reasons. First, CUSUM is a non-parametric technique which means training traffic is not required to detect the change in the traffic such as Kolmogorov complexity [33], Granger Causality Test (GCT) and Auto Regressive Model (AR Model) [34]. Second, CUSUM requires less computational and storage resources comparing to other statistical techniques. It only requires defining bounds and threshold value to detect the change in the traffic behavior. Defining the bounds and threshold depends on type of running service and traffic.

TABLE I. SIGNATURE AND ANOMALY BASED COMPARISON

Method	Detection time	Reliability	Detect new attacks	False Positive	Requirements
Signature	Fast	Yes	No	Very low	Well-known signature
Anomaly	vary	Yes	Yes	High	Trained data

VII. CONCLUSION

DoS/DDoS is one of the main security threats in the Internet. Defending against DoS/DDoS becomes a necessary step that must be considered by the companies and ISPs. DoS/DDoS detection is regarded to be one of the main phases in overcoming the DoS/DDoS problem. IDS is used to detect different types of intruders including DoS/DDoS attacks. An overview and broad classification IDS are presented. The difficulties and characteristics of DoS/DDoS attacks are discussed in the DoS detection section. Furthermore, a classification of DoS attacks is explained. Three different classifications have been chosen and divided in two groups: general DoS classification and network flooding DoS-based. In each classification, many different proposed techniques are introduced and reviewed to point out the limitations. A key observation of the authors is that while signature-based detection has limitations it should not be ignored as it is relatively efficient. In terms of the statistical techniques for anomaly-based detection, the CUSUM approach has many advantages over more sophisticated statistical instruments in that it is non-parametric and thus training is more straightforward.

REFERENCES

[1] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, pp. 39-53, 2004.

[2] J. McHugh, A. Christie, and J. Allen, "Defending yourself: The role of intrusion detection systems," Software, IEEE, vol. 17, pp. 42-51, 2000.

[3] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," 2002, pp. 255-264.

[4] T. M. Wu, "Intrusion Detection Systems " Information Assurance Technology Analysis Center (IATAC), Septemper 2009.

[5] J. P. Anderson, "Computer security threat monitoring and surveillance," 1980.

[6] D. E. Denning, "An intrusion-detection model," Software Engineering, IEEE Transactions on, pp. 222-232, 1987.

[7] M. V. Mahoney and P. K. Chan, "Learning nonstationary models of normal network traffic for detecting novel attacks," 2002, pp. 376-385.

[8] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, vol. 31, pp. 805-822, 1999.

[9] A. Sperotto, et al., "An overview of IP flow-based intrusion detection," Communications Surveys & Tutorials, IEEE, vol. 12, pp. 343-356, 2010.

[10] F. Dressler, G. Munz, and G. Carle, "Attack detection using cooperating autonomous detection systems (CATS)," Wilhelm-Schickard Institute of Computer Science, Computer Networks and Internet, 2004.

[11] S. A. Khayam, et al., "A survey of anomaley-based intrusion detection systems," School of Electrical Engineering and Computer Science (SEECS), National University of Sciences & Technology (NUST)2009.

[12] N. Ye, Secure computer and network systems: modeling, analysis and design: Wiley, 2008.

[13] R. W. Stevens, TCP/IP illustrated, Volume 1: The protocols: Addison-Wesley Professional, 1994.

[14] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, pp. 18-28, 2009.

[15] ArborNetworks, "Worldwide Infrastructure Security Report," Feb 2012.

[16] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," ACM Computing Surveys (CSUR), vol. 39, p. 42 pages, April 2007.

[17] Y. You, M. Zulkernine, and A. Haque, "Detecting flooding-based DDoS attacks," 2007, pp. 1229-1234.

[18] R. Naraine. Massive DDoS attack hit DNS root servers [Online]. Available:http://www.esecurityplanet.com/trends/article/0,10751,1486981,00.html.

[19] M. Prince. Deep Inside a DNS Amplification DDoS Attack [Online]. Available:http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack

[20] T. M. Gil and M. Poletto, "MULTOPS: a data-structure for bandwidth attack detection," in Proceedings of 10th Usenix Security Symposium, 2001, pp. 23-38.

[21] R. R. Kompella, S. Singh, and G. Varghese, "On scalable attack detection in the network," in Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement. ACM Press, , New York, 2004, pp. 187-200.

[22] G. Cheng, "Malware FAQ: Analysis on DDOS tool Stacheldraht v1. 666,"[Online].Available:http://www.sans.org/resources/malwarefaq/stacheldraht. php, 2006.

[23] T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring," NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, pp. 771-782, 2004.

[24] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," 2002, pp. 293-304.

[25] R. Talpade, G. Kim, and S. Khurana, "NOMAD: Traffic-based network monitoring framework for anomaly detection," in Fourth IEEE Symposium on Computers and Communications, 1999, pp. 442-451.

 ISBN: 978-1-61208-231-8

[26] Y. Kim, J. Y. Jo, and K. K. Suh, "Baseline profile stability for network anomaly detection," International Journal of Network Security, vol. 6, No.1, pp. 60–66, Jan 2008.

[27] V. Jacobson, "Congestion avoidance and control," in Proceedings of SIGCOMM'88, ACM, 1988, pp. 314-329.

[28] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in In Proceedings of IEEE INFOCOM, 2002, pp. 1530–1539.

[29] M. Basseville and I. V. Nikiforov, Detection of abrupt changes: theory and application vol. 15: Prentice Hall Englewood Cliffs, 1993.

[30] R. B. Blazek, H. Kim, B. Rozovskii, and A. Tartakovsky, "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch-sequential change-point detection methods," 2001, pp. 220-226.

[31] C. M. Cheng, H. Kung, and K. S. Tan, "Use of spectral analysis in defense against DoS attacks," 2002, pp. 2143-2148 vol. 3.

[32] A. B. Kulkarni, S. F. Bush, and S. C. Evans, "Detecting distributed denial-of-service attacks using Kolmogorov complexity metrics," TR176, GE Research Center, 2001.

[33] M. Li and P. M. B. Vitányi, An introduction to Kolmogorov complexity and its applications: Springer-Verlag New York Inc, 2008.

[34] J. B. D. Cabrera, et al., "Proactive detection of distributed denial of service attacks using mib traffic variables-a feasibility study," 2001, pp. 609-622.

[35] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," Internet Computing, IEEE, vol. 10, pp. 82-89, 2006.

[36] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Transactions on Computer Systems (TOCS), vol. 24, pp. 115-139, 2006.

[37] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in Proceedings of DARPA Information Survivability Conference and Exposition, 2003, pp. 303-314 vol. 1.

[38] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, New York, NY, USA, 2002, pp. 71-82.

[39] W. Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2: Addison-Wesley Longman Publishing Co., Inc., 1998.

 ISBN: 978-1-61208-231-8