Detection Techniques against DDoS Attacks: A Comprehensive Review

Shaveta Gupta
Information Technology
PGGC-11
Chandigarh,India

Dinesh Grover, Ph.D
Ex-*Director*
Deptt of CSE and IT
LLRIET,Moga

Abhinav Bhandari
Asstt Professor
Deptt of Computer Science and Engg
Punjabi University, Patiala

ABSTRACT
Distributed Denial of Service (DDoS) attacks have also become a problem for users of computer systems connected to the Internet. So defending internet from these attacks has become the need of the hour. There are three solutions against DDoS attacks: Prevention, Detection and Reaction. Detection is one of the key steps in defending against DoS/ DDoS attacks. There are some challenges that has to face while adopting any of the detection technique. If attacks can be detected close to attack sources, attack traffic can be filtered before it wastes any network bandwidth. A good detection technique should have short detection time, low false positive rate, low false negative rate but high normal packet survival ratio. This review paper provides the comparative analysis of various detection techniques with their corresponding advantages and disadvantages.

General Terms
DDoS Detection, Anamoly Based detection, Signature Based Detection.

Keywords
DDoS Attacks, False positive rate, DetectionTechniques.

1. INTRODUCTION
The DDoS attack is performed to deplete the resource of one or more victims and make it unavailable to the victim's legitimate client. Therefore it involves dumping packets from many zombies (compromised computers) towards the victim server. The server is never compromised, the databases never viewed, and the data never deleted. Throughout and after the attack, the server remains intact and compromise 'A' of CIA (Confidentially, Integrity, Availability). Backbone of this kind of attack is the network of zombies called as decoy network or botnet. Even though zombie is termed as a secondary victim it is not the target of the DDoS attack but they act as the accomplice. In this study the zombie is coined as accomplice because at law, an accomplice is a person who participates in the commission of a crime, even though they take no part in the actual crime, such is also a punishable offence. The zombies though they not initiate the attack but they participate in the DDoS attack, therefore they are accomplice. Mostly the computers are compromised due to the lack of knowledge in security issues and lack of adequate security measures. The ignorance of zombies not only leaves room for DDoS attack but their own vital, private and sensible data are under risk of being exploited by the attacker at any time. DoS attacks can generally be classified as either a Flood Attack or a Malformed (or crafted) Packet Attack and that where attacks originate simultaneously from several compromised sources and these can be classified as Distributed DoS attacks.

2. DDOS DEFENSE: CLASSIFICATION
There are different classification criteria against DDoS defense mechanisms. The first classification criteria is the location where the defense mechanism is implemented (i.e., Deployment location).The second criterion for classification is the point of time when the DDoS defense mechanisms should act in response to a possible DDoS attack. Figure 1 shows the various defense mechanisms based on different criteria:

A) Classification based on deployment location
A.1) Defence mechanisms against network/transport level DDoS attacks:

- *A.1.1) Source based mechanisms (centralized):* Source-based mechanisms are deployed near the sources of the attack to prevent network customers from generating DDoS flooding attacks[14]. These mechanisms can take place either at the edge routers of the source's local network or at the access routers of an Autonomous System (AS) that connects to the source edge routers. Various source-based mechanisms have been designed to defend against DDoS flooding attacks at the source like: Ingress/Egress filtering, MULTOPS, TOPS MANAnet's Reverse Firewall.
- *A.1.2) Destination-based mechanisms (centralized):* In the destination-based defense mechanisms, detection and response is mostly done at the destination of the attack (i.e., victim)[11]. There exist various destination-based mechanisms that can take place either at the edge routers or the access routers of the destinations AS. These mechanisms can closely observe the victim, model its behavior and detect any anomalies. Some of the major destination-based DDoS defense mechanisms are: IP Traceback mechanisms, Packet marking andfiltering mechanisms, Management Information Base (MIB), Hop-count filtering and Packet dropping based on the level of congestion.

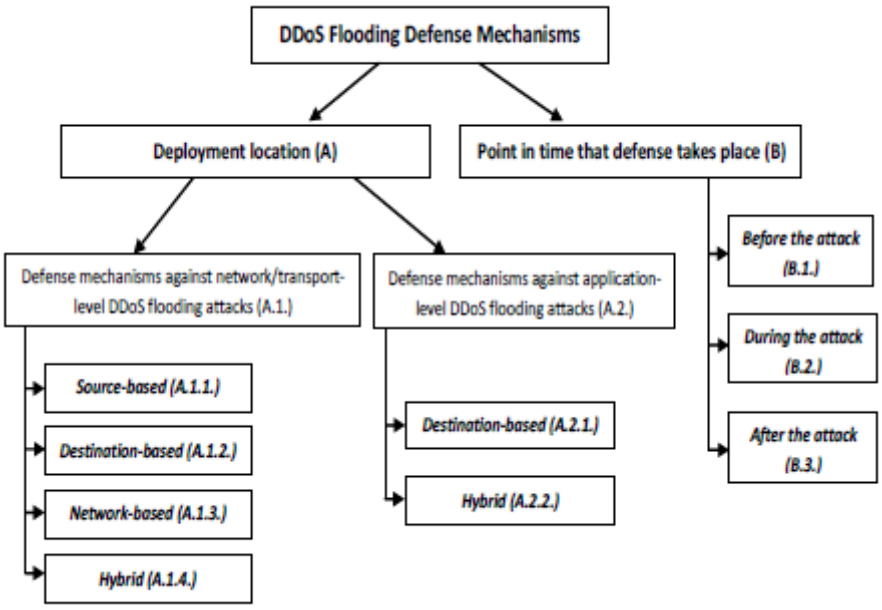

Figure 1. A taxnomy of defense mechanisms against DDoS attacks

• *A.1.3) Network-based mechanisms (centralized):* These mechanisms are deployed inside networks and mainly on the routers of the AS. Detecting attack traffic and creating a proper response to stop it at intermediate networks is an ideal goal of this category of defense mechanisms. Some of the main network-based DDoS defense mechanisms are: Route based packet filtering, detecting and filtering malicious routers.

• *A.1.4) Hybrid mechanisms (distributed):* In most of the previously discussed categories of DDoS defense mechanisms (source-based, destination-based, and network-based), there is no strong cooperation among the deployment points. Furthermore, detection and response is mostly done centrally either by each of the deployment points (e.g. source-based mechanisms) or by some responsible points within the group of deployment points (e.g. network-based mechanisms). As opposed to centralized defense mechanisms, hybrid defense mechanisms are deployed at (or their components are distributed over) multiple locations such as source, destination or intermediate networks and there is usually cooperation among the deployment points. For instance, detection can be done at the victim side and the response can be initiated and distributed to other nodes by the victim. Some of the hybrid DDoS defense mechanisms are: Hybrid packet marking and throttling/filtering mechanisms DEFCOM, COSSAC, Internet Traffic Filtering, StopIt. Table 1. compares the defense mechanism based on deployment locations.

2) Defense mechanisms against application-level DDoS attacks:

Table 1.Comparison of defense mechanism based on deployment locations

	Accuracy	Scalability	Performance	Complexity	Holistic defence
Source - based	Low	Low	Moderate	Low	No
Destination-based	High	Low	Good	Low	No
Network-based	Low	Medium	Moderate	Medium	N
Hybrid-based	Medium	Medium-High	Poor-Moderate	Medium-High	Ye

• *A.2.1) Destination-based (Server-side)mechanisms:* These defense mechanisms are deployed at the destination of the attack (i.e., victim), which is the server of the application layer protocols. Some of these major mechanisms against application-level DDoS attacks are as: Defense against Reflection/Amplification attacks, DDoS shield, Anamoly detection based on hidden semi-markov model, DAT.

• *A.2.2) Hybrid mechanism(Distributed):* These defense mechanisms employ collaboration/cooperation between clients and servers to detect and respond to the attacks. For instance, detection is done at the victim (web server/reverse proxy) and the response is initiated and distributed to the client sides by the victim. Some of the hybrid mechanisms against application-level DDoS flooding attacks are: Speak-up, DOW, Differentiate DDoS flooding bots from human, Admission control and congestion control, TMH, Hybrid detection based on trust and information theory based metrics. Table 2 shows advantages, and disadvantages of defense mechanisms against network/transport-level DDoS attacks based on their deployment location.

Table 2: Advantages, and disadvantages of defense mechanisms against network/transport-level DDoS Attacks based on their deployment location

Different locations for performing DDoS	**Advantages**	**Disadvantage**
Hybrid Defense mechanism (Distributed)	1 .More Robust against DDoS attacks.	1. Complexity and overhead because of cooperation and communication among distributed components scatterd all over the internet.
	2. More resources at various levels are available to tackle DDoS attacks.	2. Lack of incentives to the service provider to cooperate/collaborate.
		3. Need trusted communication among various distributed components in order to cooperate/coordinate.
Victim End Defence mechanism (Centralized)	1. Easy because of high rate resource consumption.	1. Network bandwidth often gets overwhelmed.
	2. Most Practically applicable type of defence scheme as web server providing critical services always try to secure their resources for legitimate users.	2. This approch detect attack only after it reaches victim and detecting an attack when legitimate clients have already been denied is not useful.
Source End Defence mechanism (Centralized)	1. Best possible defence.	1. Not Easy
	2. Prevents possibility of flooding not only on victim side but also in whole intermediate network.	2. Sources are widely distributed and sources behave almost similarly as in normal traffic.
		3. It is difficult to differentiate between legitimate and attack traffic near the sources, since the volume of the traffic may not be big enough as the traffic typically aggregates at points closer to the destinations.
		4. Difficult of deploy system at source end.
		5. The motivation for deployment of the source-based mechanisms is low since it is unclear who (i.e., customers or service providers) would pay the expenses associated with these services.
Intermediate network Defence mechanism(Centralized)	1. Detection and Traceback of attack sources are easy in this approch.	1. Deployability as to achieve full detection accuracy, all routers on internet will have to employ this detection scheme. Full practical implementation of this scheme is difficult.
	2. Aims to detect and respond to the attack in the intermediate network and as close to the source as possible.	2. High storage and processing overhead at the routers.

B) Classification by the point in time which defence takes place:

- *B.1) Before the attack (Attack Prevention):* The best point in time to stop a DDoS attack is at its launching stage. In other words, attack prevention is the best DDoS defense solution. The prevention mechanisms can be deployed at the attack sources, intermediate networks, destinations or a combination of them. Most of the prevention mechanisms aim to fix security vulnerabilities (e.g., insecure protocols, weak authentication schemes, and vulnerable computer systems) that can be exploited to launch DDoS attacks. There are some general prevention mechanisms that should be employed almost everywhere (e.g., servers, hosts, and intermediate networks) and in as many places as possible by both end hosts and service providers. Some of these general prevention mechanisms are: Fail-safe protection, resourse allocation and accounting, reconfiguration mechanisms, installing firewalls etc.

- *B.2) During the Attack(Attack Detection):* The next step in defending against DDoS attacks is attack detection, which happens during the attack. The detection mechanisms can also be deployed at sources, intermediate networks, destinations or combination of them.

- *B.3) After the attack(Attack identification and response):* After a DDoS attack is detected, the defense system should identify the source of the attack and block the attack traffic[14]. Today, most of the DDoS response mechanisms cannot completely prevent or stop DDoS attacks. Thus minimizing the attack impact and maximizing the availability of services is the main focus of all after the attack mechanisms. In this paper our main focus is on detection techniques. So we ellaborate the various detection techniques.

3. ATTACK DETECTION AND WHY IT IS DIFFICULT

- It is easy to mistake legitimate traffic as attack traffic. Therefore it is challenging to accurately detect attacks quickly and close to the attack sources.

- It is important to differentiate DoS attacks from "Flash Crowds" so that targets can react to them separately.

- These techniques are not very flexible because they are typically customized for known attack patterns.

- A large number of detection techniques use traffic logs to identify attacks. However traffic logs generate a large amount of data even during normal operation so it is difficult and time consuming to scan traffic logs looking for patterns when the network is under attack[5].

4. MEASURES FOR ATTACK DETECTION

- **A) Detection Time***:* It is how much time a detection system needed to identify the attack packets. A good detection technique should have a short detection time.

- ***B)*** **Normal Packet Survival Ratio:** It is the percentage of normal packets that can make their way to the victim in the midst of a DDoS attack. An effective packet filtering mechanism should be able to achieve a high NPSR during a DDoS attack.

- **C) False Positive Rate:**

False Positive Rate = Number of packets classified as attack packets(positive)by detection system that are confirmed to be normal(negative)

Total number of confirmed normal packets

A good detection technique should have low false positive rate.

- **D) False Negative Rate:**

False Negative Rate = Number of packets classified as normal(negative) by detection system that are confirmed to be attack(positive)

Total number of confirmed attack packets

A good detection technique should have low false negative rate.

5. CLASSIFICATION OF DETECTION TECHNIQUES

There are broadly two categories of detection techniques and their classification has been discussed in Figure 2:

A) Anamoly Based Detection: This detection system first creates a baseline profile of the normal system, network or program activity. Thereafter any activity that deviates from the baseline is treated as a possible intrusion. This detection system is proactive and autonomous and can ensure security without any

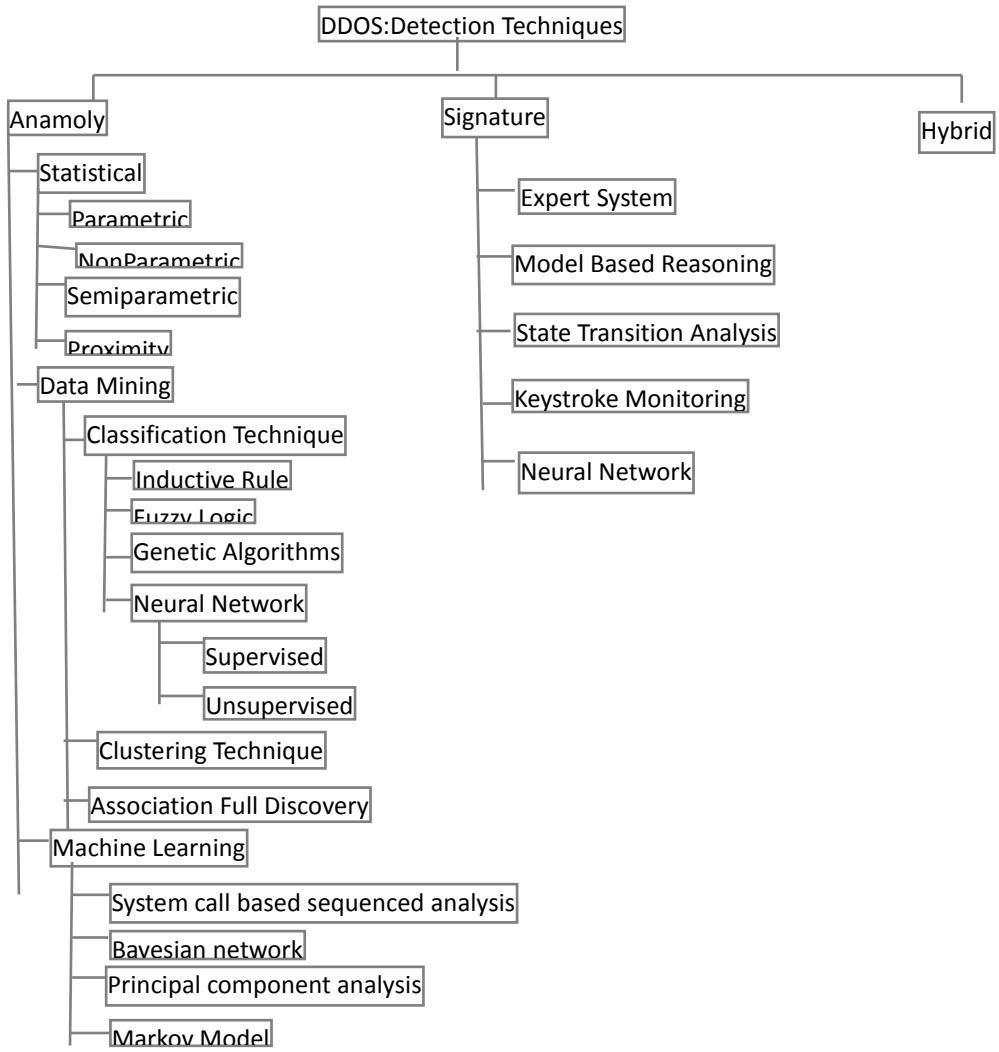

Figure 2: Classification of Detection Techniques

manual interference. An anamoly detection approach usually consistes of two phases: a training phase and testing phase. In the former, the normal traffic profile is defined; in the latter, learned profile is applied to the current traffic to look for any deviations. A number of anomaly detection mechanisms has been proposed recently to detect such deviations, which can be categorized into statistical methods, data-mining methods and machine learning based methods.

A.1)Statistical Technique: In this technique the system observes the activity of subjects and generates profile to represent their behavior. Typically two profiles are maintained for each subject: the current profile and stored profile. As the system/network events are processed, the intrusion detection system updates the current profile and periodically calculates an anamoly score by comparing the current profile with the stored profile using a function of abnormality of all measures within the profile. If the anamoly score is higher than a certain threshold the intrusion detection system generates an alert.

- *A.1.1)Proximity-based Techniques:* These techniques are simple to implement and make no prior assumptions about the data distribution model[9]. They suffer exponential computational growth as they are found on the calculations of the distance between all records.

- *A.1.2)Non-parametric Methods:* These approaches may be applicable for outlier detector where all data is accumulated beforehand and may be processed to determine parameter settings or for data where the distribution model is known. Non parametric approach in contrast are more flexible and autonomous.

- *A.1.3)Parametric Methods:* Parametric methods allow the model to be evaluated very rapidly for new instances and are suitable for large data sets; the model grows only with model complexity not data size. However, they limit their applicability by enforcing a pre-selected distribution model to fit the data. If the user knows their data fits such a distribution model then these approaches are highly accurate but many data sets do not fit one particular model. Minimum volume ellipsoid estimation and convex peeling approach come under these method.

- *A.1.4) Semi-Parametric Method:* Semi-parametric methods apply local kernel models rather than a single global distribution model. They aim to combine the speed and complexity growth advantage of parametric methods with the model flexibility of non-parametric methods.

A.2) Machine learning: It can be defined as the ability of a program or a system to learn and improve their performance on a certain task or a group of tasks over time. Unlike statistical approaches which tend to focus on understanding the process that generated the data, machine learning technique focus on building a system that improves its performance based on previous results. Much outlier detection has only focused on continuous real-valued data attributes there has been little focus on categorical data. John (1995) and Skalak and Rissland (1990) use a C4.5 decision tree to detect outliers in categorical data and thus identify errors and unexpected entries in databases. Decision trees are robust, do not suffer the curse of dimensionality as they focus on the salient attributes, and work well on noisy data. Another machine learning technique exploited for outlier detection is rule-based systems which are very similar to decision trees as they both test a series of conditions before producing a conclusion. In fact rules may be generated directly from the paths in the decision tree. Rule-based systems are more flexible and incremental than decision trees as new rules may be added or rules amended without disturbing the existing rules.

A.3) Data Mining: To eliminate the manual and adhoc elements from the process of building an intrusion detection system ,data mining approach is used. Data mining is ability to take data as input and pull from it patterns or deviations which may not be seen easily to the naked eye.

- *Classification based intrusion detection:* An intrusion detection system that classifies audit data as normal or anomalous based on a set of rules, patterns or other affiliated techniques can be broadly defined as classification based intrusion detection system. A variety of classification techniques have been proposed like inductive rule generation techniques, fuzzy logic, genetic algorithms and neural networks.

- *Clustering and outlier detection:* Clustering is a technique for finding patterns in unlabelled data with many dimensions. Clustering and outlier detection are closely related. There exist two approaches to clustering based anamoly detection. In the first approach the anamoly detection model is trained using unlabelled data that consists of both normal as well as attack traffic. In the second approach, the model is trained using only normal data and the profile of normal activity is created.

- *Association rule discovery:* These have been successfully used to mine audit data to find normal patterns for anamoly detection. Two important concepts when dealing with association rules are role confidence and rule support.

Table 3: Advantages and Disadvantages of different approaches of sigantaure based detection system

Approaches to Misuse detection	**Defination**	**Advantages**	**Disadvantages**
Expert System	Expert System Code Knowledge about attack as if-then implication rules.	1. Separation of Control Reasoning from formulation of problem solution .	1. Working memory elements that match the left side of productions to determine eligible rules for firing are essentially sequence-less.
		2. Symbolically deduce the occurrence of intrusion based on available data.	2. Software engineering concern with maintenance of knowledge base and quality of rules, which can be as good as human devising them.
			3. It is difficult to efficiently specify an order in which to match facts within natural framework of expert system shell.
Model Based Reasoning System	Combines models of misuse with evidential reasoning to support conclusions about occurrence of misuse.	1. Its basis is mathematically sound theory of reasoning in presence of uncertainty.	1 .It places additional burden on person creating intrusion detection models to assign

			meaningful and accurately evidence numbers to various parts of graph reprenting intrusion model.
		2. Structuring of planner provides independence of representation of underlying audit trail system.	2. It is also not clear from model how behaviour can be compiled efficiently in planner and its effect on detection.
		3. Potential of reducing substantial amount of processing per audit record.	
State Transition Analysis	Represents attack as a sequence of state transitions of monitored system.	1. Not limited to single audit trail.	1.Complex specification of condition.
Keystroke Monitoring	Use user keystroke to determine the occurrence of attack.		1.Without semantic analysis of contents aliases can easily defeat this technique.
Neural Network	Provides potential to identify and classify network activity based on limited incomplete and non linear data sources.	1. Flexibility.	1. Training requirements of neural network.
		2. Neural Network would be capable of analyzing data from network even if data is incomplete or distorted.	2. Training data and training methods that are used are critical.
		3. Inherent speed of neural network.	3. Black Box nature of neural network.
		4. Predictive capability to detect of instance of misuse.	4. Quantity of sensitive information is difficult to obtain.

Table 4. Advantages and Disadvantages of Anamoly based and Signature based detection techniques

Detection Techniques	Advantages	Disadvantages
Anamoly Based Detection	1. Ability to detect unknown attacks.	1. Intrinsic complexity of a system.
	2. Ability to detect "zero day attack".	2. High % of False Alarms, because it is difficult for training data to provide all types of normal traffic behavior. As a result legitimate traffic can be classified as attack traffic
	3.Ability to detect inside attacks.	
	4.As Aformentioned profiles of normal activity are customized for every system, therefore making it very difficult for attacker to know with certainity what activities it can carry out without getting detection.	3. Miscreants who know that they are being monitored can train such systems over length of time to point where intrusive behaviour is considered normal.
		4. This detection system have not gained popularity yet, they have remained a topic of an ongoing interest among research community.
Signature(Misuse)Based Detection	1. Attacks can be detected fairly reliable.	1. Required signature to be defined for all possible attacks. So requires frequent updates to keep the signture database up-to-date.
	2. Low % of False Alarms.	
	3. Comparetively simpler .	2. Maintaining state information of signatures in which an intrusive activity spans multiple discrete events—that is the complete attack signature spans multiple packets.
	4. Easy for the system administrator to determine exactly which attacks the system is currently experiencing.	
	5. This detection system begins protecting the computer/network immediately upon installation.	
	6. This detection system has a commercial success.	

B) Signature or Misuse Detection: It is a technique for intrusion detection that relies on a predefined set of attack signature. By looking for specific patterns, the signature detection based intrusion detection systems match incoming packets to the signatures of known attacks[6]. So legal or illegal behavior can be defined and compared with observed behavior [8]. Siganture based detection system are reactive. There are number of signature based detection approaches are proposed like expert system, model based reasoning, state transition analysis, key stroke monitoring and neural networks. Table 3 shown above gives us advantages and disadvantages of different approaches of signature based detection system.

- *Expert System:* Expert system detector code knowledge about attack as if-then implication rules. Rules specify the condition requisite for an attack in their if part. When all the conditions on left side of rule are satisfied the actions on right side of rule are performed which may trigger the firing of more rules or conclude the occurrence of intrusion.

- *Model Based Reasoning System:* This system combines models of misuse with evidential reasoning to support conclusions about occurences of misuse. There is database of attack scenarios, where each scenario is comprise a sequence of behaviour making up attack. At any moment system is considering a subset of these attack scenarious as likely one experienced by system.

- *State Transistion Analysis:* This represents attacks as a sequence of state transition of monitored system.

- *Keystroke Monitoring:* This approach use user keystroke to determine the occurrence of attack. Primary means is to pattern match for specific keystroke sequence inductive of attack.

- *Artificial Neural Network:* This approach provide potential to identify and classify network activity based on limited, incomplete and non linear data sources[7]. Table 4 discribes the advantages and disadvantages of Anamoly- based and Signature- based detection techniques and Table

- 5 Compares the Signature- based and Anamoly-based detection techniques based on measures like Detection time,Reliability etc.

Table 5. Signature based and Anamoly Based Detection Comparison

Method	**Signature**	**Anomaly**
Detection time	Fast	Vary
Reliability	Yes	Yes
Detect new attacks	No	Yes
False Positive	Very-Low	High
Requirements	Well-Known Signature	Trained Data

C) Hybrid systems: This approach consists of both anamoly as well as signature detection techniques strategies. In such a hybrid system the anamoly detection technique aids in the detection of new or unknown attacks while the signature detection technique detects known attacks. EMERALD is a hybrid system that ws developed in the late 1990's at SRI. The architects of EMERALD employed an esemble of techniques like statistical analysus engines and expert systems.

6. CONCLUSION

DoS/DDoS is one of the main security threats in the Internet. DDoS detection is regarded to be one of the main phases in overcoming the DoS/DDoS problem.This review paper, describes a comprehensive classification of various DDoS defense mechanisms based on deployment location and point in time that defence takes place along with their advantages and disadvantages. An ideal comprehensive DDoS defense mechanism must have specific measures like Low False Positive Rate, Low Detection time, Low alse Negative rate, High Normal packet survival ratio. Comparison of the anamoly based detection technique and signature based detection techniques based on above measures have been described. Investigation of an accurate strategy for response to identified attacks is also a future research issue.

7. REFERENCES

[1] Stephen Specht, Ruby Lee," Taxonomies of distributed Denial of Service Networks Attacks, Tools and Countermeasures:Technical Report". CE-L2003-03 May 16,2003.

[2] Rajesh Kumar,"An Introduction to DDoS – Distributed Denial of Service attack" March 15,2011.

[3]Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao,"Survey of Network-Based Defence Mechanisms Countering the DoS and DdoS Problems" ACM Computing Surveys, Vol. 39, No. 1, Article 3, Publication date: April 2007.

[4]Rocky K. C. Chang, The Hong Kong Polytechnic University,"Defending against Flooding-Based Distributed Denial-of-Service Attacks.",Volume 40 Issue 10,Oct 2002.

[5]Amit Kulkarni and Stephen Bush,"Detecting Distributed Denial-of-Service Attacks Using Kolmogorav Complexity Metrics." 2001;http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.16.5589

[6]Sandeep kumar,"A Pattern matching model for misuse intrusion detection."Proceedings of the 17th National Computer Security Conference,1994.

[7]James Cannady,"Artificial Neural Network for MisuseDetection."1998;http://webpages.cs.luc.edu/~pld/courses/447/sum08/class9/cannady.1998.artificial_neural_networks_for_misuse_detection.pdf

[8] Animesh Patcha and Jung-Min Park," An overview of anamoly detection techniques:Existing solutions and latest technological trends."Volume 51, Issue 12, 22 August 2007, Pages 3448–3470

[9]Victoria J. Hodge and Jim austin,"A survey of outlier dtection methodologies."Artificial intelligence Review 22:85-126,2004.

[10] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon,Younggoo Han, Sehun Kim,"DDos attack detection method using cluster analysis",Volume 34 Issue 3, April 2008, Pages 1659–1665

[11]Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE,"A survey of defence mechanisms against distributed denial of service flooding attacks"IEEE Communications Survey & Tutorials accepted for publication 11 Feb,2013.

[12]Mohammed Alenezi,Martin J Reed,"Methodologies for detecting DoS/DDoS attacks against network servers."*ICSNC 2012 :* The Seventh International Conference on Systems and Networks Communication

[13]Yufeng Kou, Chang-Tien Lu, Sirirat Sinvongwattana,Yo-Ping Huang,"Survey of fraud detection techniques".Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23, 2004

[14]Monowar H. Bhuyan,H.J.Kashyap,D.K.Bhattacharya and J.K. Kalita"Detecting Distributed Denial of Service Attacks:Methods,Tools and Future Directions"www.cs.uccs.edu/~jkalita/papers/2013/BhuyanMonowarComputerJournal 2013