ABSTRACT

In today's technology world, computer and digital devices network plays an important role. Almost all organizations are dependent on digital means of information storage and communication like laptops, computers, handheld devices and routers etc. An organization has to ensure the availability of these resources from the organization's network whenever required.

Distributed Denial of Service attacks are caused due to a large data sent by multiple system/devices to a single target exhausting the resources and causing unavailability of services. Detection of such attacks has gained a great attention in current computing era. Research has shown that DDOS detection using anomaly based detection mechanism gives more accurate result than the signature based detection techniques.

In this thesis rule based intrusion detection system is used to implement anomaly based detection using dynamic engine of Snort (NIDS).

Mathematical formulation based analysis is done using a comparison of correlation and mutual information between IP packets in different time intervals.

Results have shown that Mutual information method outperforms the correlation detection techniques.

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

_____

Faraz Akhtar.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

DoS..... Denial of Service

DDoS.....Distributed Denial of Service

NIDS.....Network Intrusion Detection System

LOIC.....Low Orbit Ion Cannon

RBF.....Radial Basis Function

LVQ.....Linear Vector Quantization

RBP.....Resilient Back Propagation

DPM.....Deterministic Packet Marking

PBM.....Probabilistic Packet Marking

TCP.....Transmission Control Protocol

UDP.....User Datagram Protocol

ICMP.....Internet Control Message

Protocol

PCA.....Principal Component Analysis

HMM.....Hidden Markov Models

CPR.....Congestion Participation Rate

LDDoS.....Low rate Distributed Denial of Service

EWMA .....Exponentially-Weighted Moving

IAFV.....IP Address Feature Value

Chapter 1

Introduction

1.1 Introduction

In today's technology world, computer and digital devices network plays an important role. With time number of computer and mobile users is rising in Pakistan according to recent statistics. Internet is being utilized by over a 30 million of users in Pakistan [1]. According to the recent report, 16% internet penetration is reached in the country. Almost all organizations are using digital means of information storage and communication like laptops, computers, handheld devices and routers etc. An organization has to ensure that users can gain easy and fast access to resources like databases, applications and programs from outside the organization's network whenever required. An organization's performance is directly related to the access of its resources. It is understood that availability of information when required is important aspect of progress in today's environment. In this perspective the most vicious attack in today's world is distributed denial of service attack. In this attack, targets host resources are exhausted using multiple compromised hosts casing the DDOS attack resulting in unavailability of services. DDoS attacks detection is the primary subject of this thesis.

This chapter gives an overview of basic concepts of flooding DDOS attacks, network intrusion detection systems, their types and limitations of rule based detection engines and overview of existing DDOS detection techniques.

After delivering the prerequisite knowledge and concepts, the aim, motivation, scope and contributions have been explained. Finally organization of rest of the thesis is given.

1.2 DDoS Attacks

DDoS attack impacts directly information availability requested by the user. The information can be webpages, online mobile applications and services like gaming etc. importance of information availability is realized when it becomes unavailable for a period of time or when required. Unavailability of an organization resources or application can lead to reputational as well as financial loss.

In August 1999 a very extensive and large scale DDOS attack was faced by the University of Minnesota in in which bots were used collectively to flood network devices. These attacks still exists and are increasing exponentially [2]. From last 2 years DDos Attacks is among the top 10 network attack methods from last four years [3]. In 2013, Spamhaus' website was became victim of a huge 300 Gbps DDoS attack. Later, US and EU based servers were effected by a 400 Gbps DDoS attack, in 2014[4].

1.2.1 Classification of DDoS Attacks

DDos attacks is very generic terminology. Following are three categories of DDOS attack [5][7][8].

1.2.1.1 Bandwidth-Depletion DDoS attacks

Main target of this type of attack is to consume all network resources by targeting the network devices making them unavailable to connect. In this attack a huge amount of data packet are sent to server from multiple resources making system services unavailable to the legitimate users.

1.2.1.2 Application DDOS

Application DOS is performed by exploiting a known or zero day vulnerability in an application (operating systems). In this kind of attack, attacker establishes a full TCP connection just as legitimate user. Application layer DDoS are very difficult to detect as they are launched after connection establishment with destination but are easy to defend [81].

1.2.1.3 Flooding DDoS Attacks

These kind of DDoS attacks are very common and difficult to detect. It involves sending huge legitimate requests to victim servers, either by original or forged source addresses. Legitimate access to the resources is blocked as the servers are already busy in responding to the packets sent by attackers. Attack traffic in such attacks includes TCP, UDP and ICMP packets.

1.2.2 Criticality of Flooding DDoS attacks

DDoS attacks are very easy and simple to launch because of online free source traffic generation tools and the attack packet doesn't contains any of the payload to be detected using signature of the data. Main target industries for such attacks are media, software, entertainment and technology, gaming and financial services etc. [10]. Percentage of flooding DDoS attacks occurrence is very high due to its ease of attack generation. The cyber statistics [97][98]show that there has been 718% increase in DDoS over 2013. According to the annual report about DDoS attack vectors and their distribution in 2014, the highest occurring attacks are of the flooding type that mainly included ICMP (9.82%), Syn (17.69%) and UDP (10.36%) floods [10].

1.3 Network Intrusion Detection System

A hardware or software which observes network traffic for suspicious activities and/or policy mismatches and produces event reports of attack if occurred.

1.3.1 Types of NIDS

There are various types of NIDS but following are the broad categories:

1.3.1.1 Rule-based detection:

Rule based intrusion detection systems compare incoming traffic to previously stored signatures derived on the basis of set of rules or attack patterns to identify occurrence of attack traffic. Rule-based intrusion detecting systems are able to detect known and commonly occurring DDoS attacks whose signatures are already

present in their database. An alarm is raised whenever a match is discovered. NSM, Bro, and Snort are the examples of rule based intrusion detection systems [6][18][22] . As compared to anomaly based systems, such a NIDS gives lesser false alarms but is unable to identify unseen and novel attacks like flooding DDoS attacks. This will be discussed in detail in

1.3.1.2 Anomaly-based detection:

Anomaly based network intrusion detection system collects normal or legitimate users data for a certain time period. Incoming traffic is compared with normal behavior and an alarm is generated if it violates not matches. An example of such a detection system is MULTOPS [44], it uses heuristics analysis technique to measure behavior deviation by looking at different incoming packet rates. PAYL and MCPAD are other examples of anomaly based detection engines [95] [96]. Such detection engines are a step ahead of signature based network intrusion detection systems as it has the ability to detect new or zero day attacks whose rules or signatures have not been known before. However, there is high probability of false alarms. There are many ways to fine tune the results for reducing false alarm rates.

1.3.1.3 Hybrid Detection:

An intrusion detection system that involves using qualities of both signature based detection system and anomaly based detection and is known as hybrid NIDS. After examining different positive features of different anomaly based and signature based systems, this approach combines benefits of different NIDS belonging to

both types. Studies indicate that this is found to be a better approach as compared to both of them separately since it covers limitations of both.

1.4 Motivation and Problem Statement

Flooding DDoS attack incidents are rising with time causing damage to individuals, servers, websites and networks [10][97][98]. It has been used by hackers, cyber-terrorists and hacktivists because of limited detection methods against it. Highly sophisticated flooding DDoS attacks can bypass firewalls as well.

Rule-based detection is the most commonly used methodology to detect flooding DDoS attacks. The de-facto intrusion detection system, Snort is also based on the rule-based detection [75]. Unfortunately, it suffers from limitations because it cannot monitor traffic flow [94] and thus cannot detect flooding DDoS attacks efficiently as discussed in [13][14][15][16][17] .Literature has shown that most commonly used NIDS are short of detecting flooding DDoS attacks if used exclusively because they lack intelligent traffic analysis.

Since, rule-based NIDS, Snort is open-source and most commonly used, finding an appropriate countermeasure for flooding DDoS attacks and integrating it with Snort poses a great challenge for organizations worldwide. It is utmost need of today's growing dependence on internet to detect such attacks timely, accurately and efficiently. The problem statement is "**There is a need to explore and analyze the detection capability of flooding DDoS attacks in rule-based NIDS with the analyses of the extent to which existing techniques detect those attacks and**

introduce a flooding DDoS attack detection technique that outperforms the existing detection methods".

1.5 Flow Based DDoS Detection Techniques

Flow based detection technique is new enhancement to DDoS protection. A flow is a unidirectional data stream where all packets share some or all of these features: IP source address and destination address, source and destination port and protocol value [20][62]. The idea of this technique is basically to use only a part of information as above mentioned features of incoming packets and examine this information by combining the incoming packets in the form of flows. Studies have indicated that flow detection is much more reliable than a solution relying on rule based signature database. Such a mechanism tracks all packets thus consuming memory resources much more that flow based mechanism [21]. Flow detection techniques consume lesser resources as they track only header information from the incoming packets. Also they have the ability to detect novel DDoS attacks better than payload based detection mechanisms [13][14][15][16][17][60]. Rule Based NIDS will become more reliable if such method are integrated with it before its detection engine.

1.6 Aims & Objectives

Primarily goals to achieve in this thesis are following:

1. Analysis of existing flooding DDoS attack detections techniques that detect such accurately and reliably.

2. Development of efficient flooding DDoS attack detection method.
3. Integration of flow based DDoS detection techniques with rule-based NIDS, the flooding DDoS attacks that are missed by other means are targeted to be identified by adding the proposed capability.
4. Analysis of proposed method with respect to traditional detection technique used by rule-based NIDS generally is to be presented.

1.7 Thesis Contributions

Thesis contributions are as follows:

1.7.1 Traffic Generation

Network traffic generating tools have been used to generate and deploy flooding DDoS attack traffic and normal traffic that closely resemble real-world scenarios. A realistic traffic generation framework has been co-operatively developed as a part of this research in order to synthetically generate and deploy different attack and normal traffic scenarios. The framework makes use of modest hardware and exploits the random IP generation feature of various attack generating tools, which is used for sending network packets with multiple distinct IP addresses from a single source machine to a single destination machine.

1.7.1.1 Test-Bed Formulation

In order to analyze the algorithms under study effectively, test benche have been established using real systems.

1.7.2 Implementation of Mutual information Technique to Detect DDoS Attacks

The 3rd contribution of the thesis is the design and a proof-of-concept implementation of a DDoS attack detection technique based on Mutual information of the incoming packets over multiple sliding window time intervals. The proposed technique is an extension of the previous research conducted in this direction and has helped to minimize false negatives and false positives that are faced in the old scheme [55].

1.7.3 Integration of Improved Correlation Technique with De-Facto NIDS

The proposed technique is integrated with the de-facto rule-based NIDS as a dynamic preprocessor. To the best of our knowledge, to date, no similar technique has been introduced within the chosen rule-based NIDS for detection of flooding DDoS attack.

1.7.4 Analysis of Improved Correlation Technique

Analysis of the proposed technique has been conducted with respect to false positive and false negative alarms. It has been seen that the proposed correlation outperforms the old correlation technique and Snort shows much better results in terms of detecting flooding DDoS attacks when the improved correlation algorithm is integrated with it.

1.8 Thesis Organization

The rest of the thesis is organized as follows:

In Chapter 2, mechanism for detecting flooding DDoS attacks incorporated in rule based NIDS is evaluated and their limitation has been discussed. Then the solutions to detect distributed denial of service attacks in general and flooding DDoS attacks in particular, as proposed by other authors, will be presented and discussed.

In Chapter 4, design of flooding DDoS attack detection technique based on improved correlation technique is presented. The proposed technique extends the previous work done in this direction by [55]. They analyzed correlation coefficient of incoming network packets per two consecutive intervals and observed that the value of correlation coefficient is abnormally reduced during attack conditions; since there will be larger set of unique source IP addresses per unit time. We propose multiple sliding window time interval correlation analyses using correlations of 4 consecutive sliding windows, in order to reliably determine if the current incoming network traffic represents attack condition or not.

In Chapter 5, the test scenarios, test-beds and implementation details have been explained. Snort has been chosen as the subject NIDS as it has achieved the position of de-facto standard among all the NIDS. Two test benches have been used, one comprising of physical systems called Test-bed 1 while the other is emulation based on DeterLab called Test-bed 2. While keeping the packet per second range steady, variations in the uniqueness of source IP addresses has been

tested against both algorithms and for both test-beds; 1 and 2. Tests have been done on attack traffic as well as on normal traffic.

In Chapter 6, results have been presented. It has been shown from results that the proposed correlation algorithm successfully identified the attack instances in all the attacks scenarios with very low rate of false negatives and no legitimate traffic was detected as attack traffic, hence, there were no false positives at all. Therefore, the proposed correlation technique outperforms the rest of the techniques.

In Chapter 7, concluding remarks have been given. The achieved objectives have been explained in detail. Besides, the limitation and future directions have been discussed.

1.9 Conclusion

In this chapter the basics of DoS and DDoS have been covered along with their types. Criticality of detecting flooding based DDoS attack has been thrown light upon. Then, types of NIDS have been discussed and the current status of rule-based NIDS in terms of detecting flooding based DDoS attacks has been explained. The main objectives, problem and scope of the thesis have been explained.

Chapter 2

Literature Review

2.1 Introduction

In this chapter we evaluate the techniques to identify flooding DDoS attacks using rule based. The characteristics and the limitation of these respective techniques have been discussed in Section 2.2. In the following section we discuss the various schemes and techniques presented by other researchers to detect and apprehend distributed denial of service attacks in general and flooding DDoS attacks in particular. The comparative analysis of these earlier schemes is exhibited in Figure 2.1. To simplify the analysis we have classified these schemes in three categories. The 'neural network based DDoS detecting schemes' requires the training of the victim system to employ defensive measures like LVO, RBF, BP and RBP. The implementation of this scheme necessitates huge memory and CPU consumption to train effectively for the attack scenarios. 'Trace back schemes' primarily focuses on detecting an ongoing DDoS attack and then mapping out the source of the attack. 'Statistical DDoS detection techniques' analyzes network traffic's nature and consumption using statistical models and metrics to determine if an attack is underway or not. Our topic of research 'Flow based detection' technique lies in this Statistical DDoS detection category. In this study, we have discussed in detail

most recent flow based detection schemes along with their respective shortcomings. In the later part of this chapter, we have presented a summary of flow based schemes in Table 2.1.

2.2 Flooding DDoS Detection Solutions in Rule-Based NIDS

In this section, the benefits and shortcomings of rule based NIDS are discussed. Rule-based NIDS operates on a technique called 'rate filtration'. This technique limits the flow of packets in order to detect and deter potential DDoS incidents. This may seem like a promising technique but a closer examination reveals that this technique falters if the number of packets sent by the malicious IP lies within the limit or threshold defined, and thus result in DDoS. The rate_filter parameters in SNORT are mentioned below [94]:

```
rate_filter \ gen_id 1, sig_id 469, \
track by_dst, \
count 25, seconds 60, \
new_action drop, timeout 30
```

These SNORT parameters generate flags if a destination or victim IP receives packets with a rate of 25 seconds, this alert has a time restriction of 30 seconds after which it automatically goes into benign state. Even tuning down the "count" parameter to 10 or 5 packets per 60 seconds is not a practical solution, as this criterion will result in prospect of generating false alerts. This will even result in black-holing the legitimate packets and flag them as malicious. The thin line between setting a threshold to deter DDoS packets and generating false negatives

is what makes it technique inefficient. This rate filter or rate limitation is the only technique featured in Snort to defend against flooding attacks and is discussed in detail in Chapter 6.

An open source rules based NIDS was presented by Cearns that featured a flooding DDoS detection preprocessor to limit the rate of incoming packets. In year 2002, a rate filter parameter was integrated in Snort's rules but its inability to distinct between legitimate and malicious traffic when exceed the defined threshold (as discussed earlier) is an issue of concern [91].

A Hybrid approach to detect DDoS attacks was proposed by Uyar et al. in [92]. He suggested the hybrid IDS that makes use of both signature-based and anomaly-based techniques to detect and deflect the DDoS attacks efficiently. The idea behind this proposal was to integrate the advantages of both technique as neither is capable to cater and detect all possible attack scenarios on their own.

In 2010 rule based NIDS was pit against LOIC to evaluate its potential against new generation DoS attacks. Low Orbit Ion Cannon (LOIC) [82] is an offensive tool that can be used to cause network stressing and denial of service. NIDS failed to mitigate this well-known despite of the fact that the signatures of LOIC were fed into it. The reason behind this failure was because LOIC had thousands of variants and NIDS need to learn them all in advance in order to protect against them. The flexibility that LOIC provided to perpetrators to specify their own content string exploited this very design specification of NIDS and made it rather ineffective. The

threshold based Rate filtering was unable to distinguish between legitimate and malicious traffic and was tricked into dropping all packets [93].

[74] discusses a study conducted in 2011 that was intended to evaluate NIDS against four types of DDoS attacks using real time traffic. This technique was successful against at lower rate of attack traffic but was ineffective when incoming packet rate was higher than 6000 packets per second [74].

2.3 Recent Flooding DDoS Detection Solutions

In this section we discuss the more recent Flooding DDoS detection solutions. We have categorized these schemes generically as illustrated in Figure 2.1.

2.3.1 Overview of Neural Networks Based Solutions

Neural networks are network equivalent of a human brain and use a set of programs to parallel process the procedures. The systems based on neural schemes use diverse rules to detect and intercept DoS attacks in real time scenarios and are fed and trained with hefty data sets.

2.3.1.1 Solutions Based on Neural Networks

In order to precisely detect and classify the attacks in public networks, Radical Basis Function (RBF) technique was proposed by Gavrilis and Dermatas in [23].

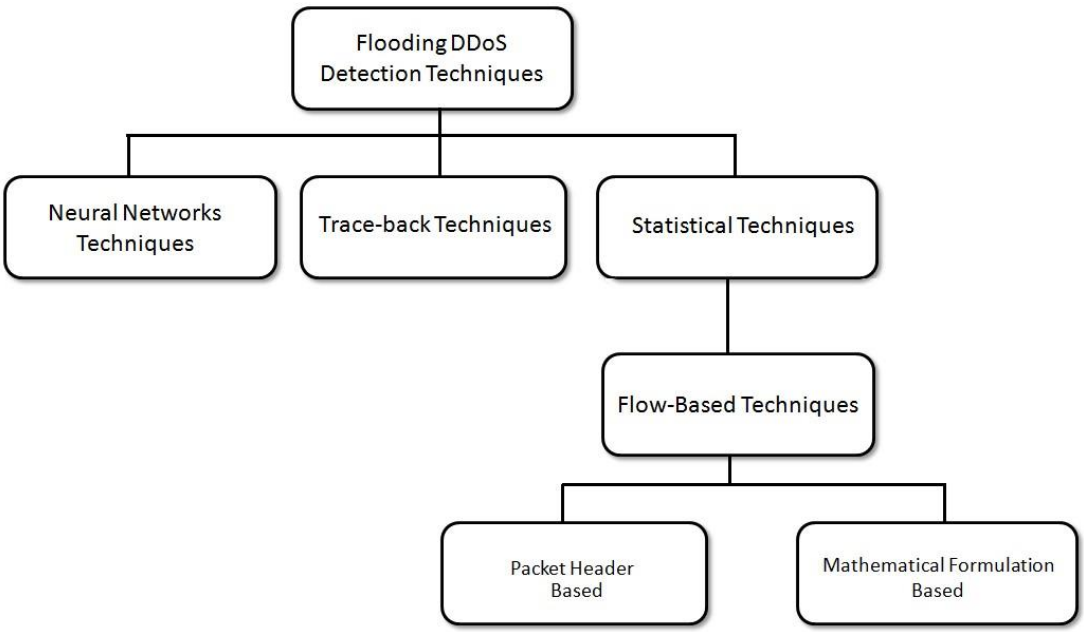

Figure 2.1: Taxonomy representing categories of solutions proposed for Flooding DDoS Detection

Li, Liu and Gu [24] proposed a neural network based model named as Linear Vector Quantization (LVQ) to detect DoS attacks. Karimazad and Faraahi [25] suggested the use of Radial Basis Function (RBF) neural networks to detect DDoS packets.

Kumar and Selvakumaar [26] suggested to use set of classifiers to detect DDoS; RBP was chosen as the base classifier for neural networks. Agarwal and Gupta [27] demonstrated to detect DDoS using back propagation scheme. This technique makes feeds sets of traffic as input and measures the number of perpetrators. Neural networks need to be trained with both normal and attack traffics so to make them intelligently efficient against DoS attacks. In [28][29] a BP model based technique was proposed to estimate the DDoS attack strength and number of zombies.

2.3.1.2 Limitations of Neural Networks

The neural network schemes have many limitations. Overall, in order to understand underlying network structure sufficiently, a neural network has to be fed with large training data set. The limitation of these schemes lies in the fact that with the increase of training data, more computational and implementation cost is required, thus making these schemes inapplicable in real time large network scenarios [30].

2.3.2 Overview of Trace-back / Attacker Pinpoint Methodologies

John and Sivakumar in [83] gave survey of various trace-back schemes and explained the general characteristics that an ideal trace-back methodology should possess. They can be summarized as: It should be able to pinpoint attacker using single packet with least memory consumption and internet service providers involvement. Besides, such scheme should not reveal the identity of the tracing machine. Such schemes must be able to trace-back the attacker no matter whatsoever transformations have been applied to the attack packet.

2.3.2.1 Solutions Based on Trace-back / Attacker Pinpoint Methodologies

Lipson in [31] proposed a trace-back scheme where ICMP massage was sent with traffic, in order to know the information of the path contained in the ICMP message. This was called ICMP messaging scheme. This ICMP messaging scheme relies on the assumption that the percentage of attack packets is more than legitimate packets but this may not be the case always specially when low rate DDoS attacks are launched. Hop by hop trace-back was proposed by Kumar, Sangal

and Bhandari in [32] in which the process of attacker identification was carried out iteratively on the routers closest to the victim system towards the attack source until the attacker's source is fully traced.

Some other trace back schemes include deterministic packet marking (DPM) in which a packet belonging to a network is marked with a unique information like the first ingress edge router or sometimes the complete route. The router embeds its IP address deterministically into the IP packets. The scheme [33] was introduced to overcome some drawbacks of probabilistic packet marking (PBM) as it has simple implementation and requires less computational overhead on intermediate routers.

2.3.2.2 Limitations of Trace-back / Attacker Pinpoint Methodologies

The trace-back schemes have their own limitations. If flooding DDoS attacks consume the whole network bandwidth, the ICMP packets might be dropped thus making it difficult to trace back the attacker. In this way the whole scheme might fail. The complexity and computational cost limitations lie with hop by hop trace back methodology.

The deterministic packet marking also comes with several drawbacks. The unique information stored as a mark is only at the first edge router, reconstruction of the route requires more packets. This makes it difficult and mostly impossible to trace the true attacker source. Besides posing computational overhead with such

schemes, in case of reflector attacks, the traced source IP will be of the innocent machines and not the original attacker.

While each scheme has its own limitations, some of the major ones are various assumptions that do not map onto real network scenarios, chances of false negatives and large computational power requirements [34].

2.3.3 Overview of Statistical Techniques

Statistical techniques are often applied for the detailed study of a given data. It collects and organizes data in an interpretable way. This procedure is called sampling. The next procedure that the statistical technique undergoes is data analyses, interpretation and presentation of results. Any aspect of data can be handled using statistical techniques.

2.3.3.1 Solutions Based on Statistical Techniques

In [38] and [39] a principal component analysis (PCA) techniques has been proposed. But studies indicate that PCA methodology used cannot detect anomalies effectively since inadequate methods are used to tune principal component analysis[40][41]. A stable profile maintenance idea was proposed in [42] that can detect sudden changes in network packets. Monitoring 15 packet attributed with use of relational analysis and decision trees was proposed in [43]. The metrics used were types of protocols, packet flag options, time to live and packet size.

Two statistical tests are proposed for detecting flooding DDoS Attacks. Firstly, it compares the differences involving the overall means of the incoming traffic arrival rate and the normal traffic arrival rate. If the difference is significant, it concludes that the traffic may include flooding attack packets [71].

A heuristic data structure was proposed to detect DDoS attacks called as MULTOPS [44]. The assumption was that during a normal scenario, the traffic between given two nodes is proportional. This leads to false alarms since any disproportional traffic will be detected as attack traffic which is not the case every time.

2.3.3.2 Limitations of Statistical Detection Techniques

Adjustment and fine tuning of PCA detection metrics used is a difficult task to accomplish [40][41]. MULTOPS leads to false alarms since any disproportional traffic will be detected as attack traffic which is not the case every time. Besides, the authors pointed out some failure points of MULTOPS when attack is launched from spoofed IPs since in that case, the assumption will never become true[64][65]. in [71] low rate DoS attacks cannot be detected because the tests only produce alarm when huge incoming traffic is seen. Profile maintenance idea came up with an assumption. Their assumption was that these four metrics are enough to detect instability in network traffic but the chosen metrics were not directly related to denial of service attacks and therefore, large amount of false alarms were faced in the technique [63].

2.3.4 Flow-Based Detection Techniques

We have classified the schemes into two categories as indicated in figure 2.1. i.e. Mathematical Formulation Based and Packet Header Feature Extraction Based

Classification. We shall discuss about the classification in detail in Chapter 3. Following are the most significant works done in the area of flow based flooding DDoS detection:

2.3.4.1 Principal component analyses (PCA) based approaches

Principal component analyses (PCA) based approaches include studies in [48] and [49]. Network DDoS attacks were proposed to be detected by traffic decomposition to normal and abnormal divisions. The division were called the sub spaces. Studies have indicated that PCA based schemes are not practically efficient to be adopted because difficulty is faced during adjustment and fine tuning of the metrics used for attack detection [40][41][69].

2.3.4.2 D-WARD

D-WARD was proposed in [70] that acted as a linking channel between the internet and the victim network. A complete record of two way traffic, i.e. each flow record between the internet and victim network had to be kept in order to identify the attacks. The record is compared with previously stored normal network statistics. A rate limitation is applied to the identified attack traffic. Studies show that D-WARD consumes more memory space than other network based detection mechanisms [72].

2.3.4.3 Spatial & Temporal Correlation

A network wide DDoS attack detection technique was proposed in [46] in which the authors claimed to detect attacks efficiently using spatial correlation for feature extraction and temporal correlation for attack detection. This study has its

own limitation because it can only detect attacks launched from spoofed IP addresses. While this is the most commonly occurring DDoS scenario, there might be real machines launching the attack with true source IP addresses [47].

2.3.4.4 Time Series Analysis Using HVM

A structural approach towards developing flow based intrusion detection system and automatic parameter tuning was proposed in [17]. A flow based time series analyses has been done for intrusion detection. For presenting the time series analysis, the authors have used Hidden Markov Models (HMMs). Unfortunately, their work has an unacceptable ratio of false positives.

2.3.4.5 IP Address Feature Value

In [59] Cheng, Yin, Liu et. al. gave a formula for IP Address Feature Value (IAFV) to detect DDoS attacks in a given flow of incoming packets. They gave a unique idea that a network flow F can be analyzed efficiently by classifying the incoming packets of the flow by source and destination IP address. The classification of packets was such that packets of one class (flow) will contain same source and destination IP addresses.

2.3.4.6 Congestion Participation Rate

In [50] flow level network traffic is used and through CPR (Congestion Participation Rate), low rate DoS (LDDoS) attacks were proposed to be detected. Unfortunately, there scheme can only detect a small range of DoS attacks that makes it insufficient to implement in real time networks.

2.3.4.7 Profile Based NfSen Plugin

In [51] a flow based SSH dictionary attacks detection mechanism is demonstrated which they implemented as a plugin for NfSen tool. The proposed algorithm defined rules set for attacks. A profile was maintained for the incoming packets based on the rule set and the packets were monitored in the form of flow, i.e. packets per flow per minute. The accuracy of their algorithm is yet needed to be investigated since the rules used to maintain profile need to be changed depending on the size of SSH attacks.

2.3.4.8 Flow Record Table Based Approaches

In [54] pattern of flow is recorded using flow table through which data is extracted and detection is made based upon already learnt pattern of DDoS flow like average packets per flow per unit time. However, the average will not give accurate results since some packets will have higher number of occurrences than the others. A blacklist is maintained for the detected packets, which in real scenarios is of no use since DDoS occurs from unique source IPs. Similar techniques are used in some other studies like in [56], per source IP table or a per flow table is maintained for detection. Maintaining table for each flow not only poses a scalability issue but also detecting the flows causing DDoS specially in case of flooding attacks arriving from spoofed IP packets becomes challenging.

2.3.4.9 Traffic Behavior Correlation Analyses

Using flow between attack and victim nodes, detection of DDoS attacks proactively was the technique proposed by [52]. Correlation of traffic behavior between

attacker and victim machines was calculated. A normal profile is maintained in order to compare the incoming packets with that profile. The main limitation of this technique is the attack methodology and attack tool used in their scheme does not map today's complex attacks. In reality, more sophisticated attacks are encountered [53].

2.3.4.10 EWMA

In [37], the authors applied exponentially-weighted moving average (EWMA) algorithm to detect changes in incoming traffic. If the intensity of the network traffic increases with time, an alarm is raised. The main issue with such techniques is that the change point detection occurs at one time series. This might result in false alarms because in some cases flash crowd events might raise the network traffic to abnormal level for particular time [65].

2.3.4.11 HiFIND

Another effort done to detect flooding attacks and port scans using flow based approach was proposed in [58]. The technique was names as HiFIND (high-speed flowlevel intrusion detection). They claimed to detect the attacks efficiently but studies have shown that their scheme was prone to huge false negatives and was unable to differentiate the attack events from flash events or network congestions [56].

2.3.4.12 Change Point Detection CUSUM Technique

Change point detection is a very well known and much researched technique used to detect flooding DDoS attacks. Many studies have proposed change point

detection algorithms. Some of them are improvements of the previous work done. Change point detection works on time series where the algorithm is applied to certain time series of the network traffic and was first proposed in [24] as CUSUM. In [35] and [36], CUSUM was used to detect SYN flooding DDoS attacks. This method is rather intricate and resource exhaustive to detect DDoS. In various studies, the stand-alone use of CUSUM is argued to be discordant for precisely detecting a DDoS. Also a higher rate of false alarms was noticed in [68]. The CUSUM method matches the inbound packets with the threshold defined and can only detect flooding events in case of higher rate of inbound packets. Hence, it is insufficient to detect general DDoS attacks [66][67].

2.3.4.13 Correlation of Incoming IP Addresses

Mapping the formula of correlation coefficient to network traffic was proposed by Zhongmin and Xinsheng in [55]. The authors performed analysis of correlation coefficient of inbound packets for two consecutive intervals and observed that the value of correlation coefficient irregularly reduces during attack. The authors called this method 'sliding window' as the sample set of attack was centered upon the correlation coefficient values per two consecutive time periods.

2.4 Summary of Flow Based Techniques

Based on reviewed literature, the existing solutions were grouped into three main categories. To date, no comprehensive solution has been proposed to identify

flooding DDoS. Major flow-based DDoS detecting solutions along with their limitations are tabulated in Table 2.1.

2.5 Conclusion

This chapter highlights all the recent solutions proposed for flooding DDoS detection that are implemented within rule-based NIDS or exclusively along with their shortcomings. Each approach has its own limitations. There is a lack of comprehensive solution that should be adaptable to wide network range, accurate in detection, gives least false alarms and effective against today's flooding DDoS attack launching tools.

Table 2.1: Summary of Flow-Based Solutions

Sr. No	Major Flow Based Proposed Scheme	Limitations
1	PCA Based Approaches[48][49]	not practical to be adopted in today's network scenario
2	D-WARD[70]	not memory efficient
3	Temporal Correlation[46]	only for spoofed attack IPs
4	Time series analyses based on HVM[17]	high false positives
5	CPR[50]	insufficient for real time implementation
6	Flow Table[54]	high false alarms, not scalable
7	EWMA [37]	cannot differentiate attack from flash events
8	Chi-Square[73]	not memory efficient
9	HiFIND[58]	high false negatives
10	Change Point Detectors [24][35][36]	high false alarms, complex, not memory efficient
11	NfSen plugin[51]	need to change profile for different attack data sets
12	Traffic Behavior Correlation Analyses[52]	insufficient for real time implementation
13	IP Address Feature Value [59]	refer to Chapter 3 and 6
14	Correlation of IP Addresses [55]	refer to Chapter 3 and 6

Proposed Solution

3.1 Introduction

In this chapter, a solution to the flooding DDoS attack detection problem is provided, and extended flooding DDoS detection strategy is deigned. Flooding distributed denial of service attacks first hit the network almost more than a decade ago [45] where a set of compromised machines/nodes were directed by their command machine (main attacker) to launch high volume of legitimate but unwanted traffic towards the victim machine. Flooding DDoS attack detection continues to represent a very hazardous threat in the internet world [81]. The issue with flooding DDoS attack detection is that the requests sent by the bots (compromised hosts) or the tools used for launching attack are legitimate so it is a challenging problem to differentiate between a legitimate traffic and attack. In this Chapter, an improved design of flooding DDoS attack detection technique based on an existing correlation technique [55] is presented. The existing correlation technique is based on of the change in rate of new source IP addresses of the incoming packets per four consecutive time intervals while the improved Mutual information technique is also based on of the rate change of new source IP addresses of the incoming packets over a sliding window time interval.

3.2 Issues in the Existing Correlation Algorithm

A large number of attack packets originating from unseen or random source IP addresses is the main indicator of a flooding DDoS attack. This was the characteristic feature taken by Correlation algorithm [55].

The Correlation algorithm uses multiple sliding window time interval as a time scale to analyze the network flow resulting in increased number of calculations. Although this algorithm solves the scalability issue; since only feature needed to be extracted in order to be fed into the system is source IP address of the packet, the MSW Correlation technique is prone to false positives.

If a burst of legitimate data packets, called flash crowd hits in that time interval, it raises the alarm and produces false positives. Also, if for that certain periods of time, the correlation value between attack packets of multiple time windows is higher than the defined threshold, no attack will be detected and thus results in false negatives.

3.3 Proposed Mutual Information Algorithm

The proposed technique has been named as Mutual information algorithm technique. In MSW- Correlation technique, correlation coefficient of incoming network packets per four consecutive sliding window time intervals was analyzed and observed that the value of correlation coefficient is abnormally reduced during attack conditions; since there will be larger set of unique source IP addresses per unit time. Hence, the determination of attack is based upon the values of correlation coefficient per four consecutive time periods, called as sliding window. An enhancement has been introduced in this technique, where sliding window time interval mutual information

analyses has been calculated using mutual information value of two consecutive sliding windows, in order to reliably determine if the current incoming network traffic represents attack condition or not.

3.3.2 Steps for Mutual Information Technique

The algorithm is explained using a flowchart in figure 4.3. Each of the step is explained as follows:

3.3.2.1 Sliding Window Time Intervals

As already discussed, in order to reliably determine if the current incoming network traffic represents attack condition or not, sliding window time interval mutual information analyses has been calculated using mutual information of two consecutive sliding windows.

Let *x* and *y* be any two consecutive time instants such that y > x.

Then: *tx,y* denotes *x-th* and *y-th* time interval between instants x and y, where y > x

And: *I* denotes the Mutual Information.

3.3.2.2 Packet Count for each Sliding Window Time Interval

For sliding window time interval t1, 2 the total number of packets coming from all source IP addresses is calculated. This will give clear statistics of how many source IP address have been received by victim in sliding window interval. Using this data along

with the unique source IP addresses count for each sliding window time interval Mutual information is calculated.

Table 3.1 shows the Mutual Information calculation process and terminologies used to describe the Mutual Information algorithm calculation.

Table 3.1: Symbols used for Mutual Information algorithm

Terminology	*Symbols/Formulas*	*Meaning*
Total IP Addresses	K	Number of IP addresses
Sliding window time intervals	$t_{1,2}$	Time interval between first and second time instants
First instance packet data	$X(i)$	Number of packets from unique IP in first instance t_1
2nd instance packet data	$X_{n+1}(i)$	Number of packets from unique IP in 2nd instance t_2
Mutual Information	$MI= \sum_{i=1}^{m} \left(\frac{X[i]}{totpacket}\right) * \log\left(\frac{X[i]}{totpacket}\right) * \left(1 + \frac{X_{n+1}[i]}{totpacket}\right)$	MI calculated for Kth IP address

Mutual information is calculated using number of packets x(i) in first sliding window time interval t_1 and number of packets received in 2nd sliding window time interval t_2.

Let the threshold for attack be denoted as MI.

Input: A network data in form of flow F, a sliding window time interval t1,2, source IP addresses xi(n)

Output: Mutual Information values

1: **For** (sliding window time interval t1,2)

2: Calculate xi(n)

\\ xi(n) is the number of packets of a unique source IP address

3: **End For**

4: **For**(all the packets)

5: Calculate x(n)

\\ Calculate the amount of all data packets in that window time interval

6: **End For**

7: **For** (each data packet in sliding window time interval t1,2)

8: Calculate s=s+ (Pr(xi(n))*log pr(xi(n))*(1+pr(xi(n+1))))

9: Calculate MI=s;

\\ correlation coefficient for t1,2

10: **End For**

Figure3.1: Mutual Information Algorithm

3.3.3 Flow-Chart for MSW-Correlation Technique

The flow chart explains the main procedures of the proposed Mutual Information algorithm. The total number of packets in each sliding window time interval is calculated, then the unique source IP addresses in each sliding window time interval is calculated. Mutual Information value is calculated for slinging window time interval. The decision is made based output MI value.

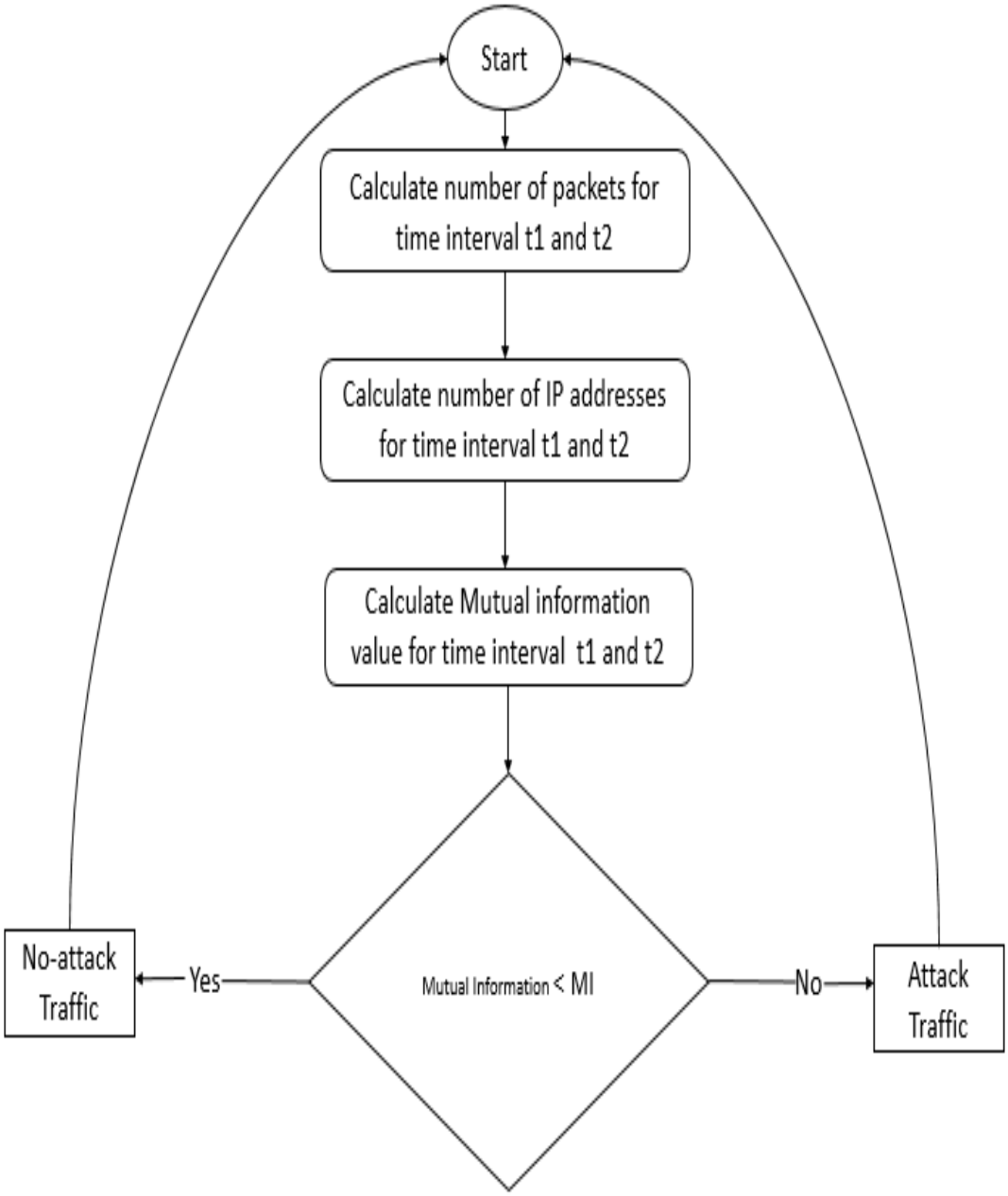

Figure 3.2: Flow Chart of Mutual Information Algorithm

3.4 Conclusion

Most of the techniques deployed are insufficient to detect flooding DDoS attacks either due to either scalability issue or structural weakness or lack of accurate detection that leads to false alarms. In this chapter, a Mutual Information based flooding DDoS detection technique is proposed, which is based on the work done in [55] and it aims to limit the false positives and false negatives. It does so by making use of multiple sliding window time intervals analyses using Mutual Information to improve the identification of malicious traffic.

Chapter 4

Implementation and Testing

4.1 Introduction

As the primary goal of this thesis is to introduce a better flooding DDoS detection technique using rule based network intrusion detection system. The network intrusion detection system Snort has been selected for the purpose as it is de-facto standard among all the NIDS. Since it is rule based, it depends upon signature present in the databases for attack detection, it is lightweight and produces expected results based on the attack packet matches in its database. Test bench utilized in the implementation of the solution is comprised of physical systems.

4.2 Snort Architecture

Snort in attack detection mode inspect the incoming packets and matches the signatures in the databases if the incoming traffic flow is legitimate it simply passes it on else generates alarms based on the rules and logs the respected event. The main packet flow for the detection in Snort engine is described in Figure.

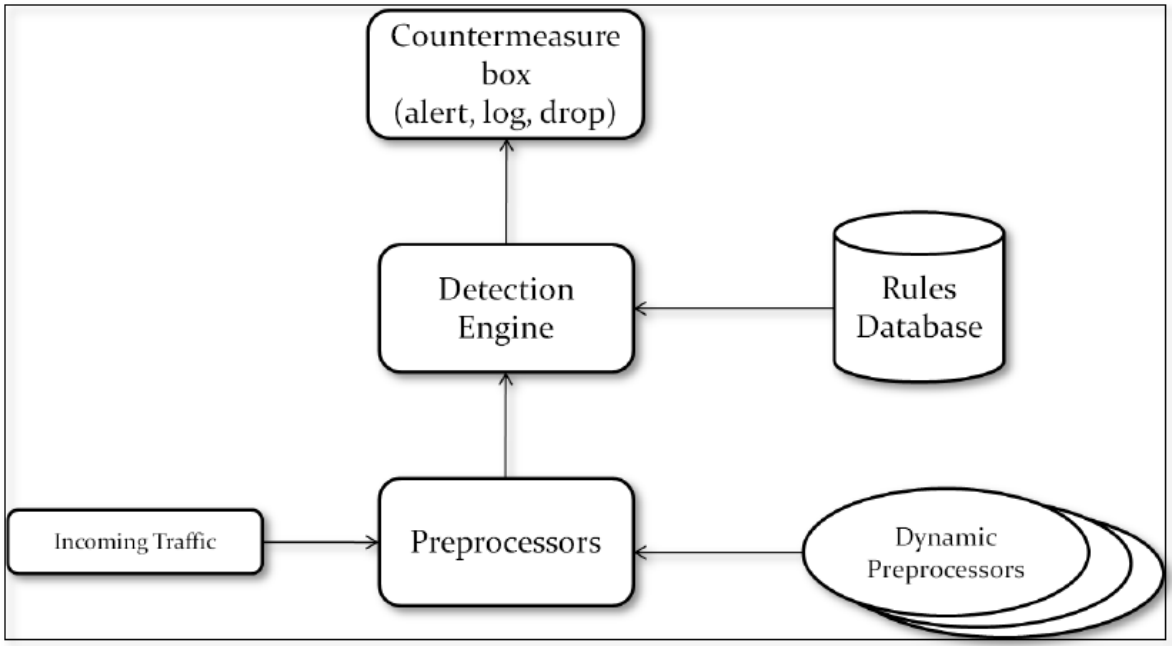

Figure 4.1: Snort Overview

4.2.1 Packet Decoder:

Packet decoder observe the protocol of incoming the incoming raw data packets from all TCP/IP layers. All of the information to be used for the detection is separated and is stored in the data structures and forwarded to the preprocessors.

4.2.2 Preprocessors:

There are various preprocessors in Snort, working for a specific attacks detection. The sequence with which each packet will be checked/processed for attack signature detection can be prioritized Snort configurations. Primary tasks carried out by preprocessors are packet fragmentation, normalization and stream reassembly. In case of legitimate traffic, data is passed on to the detection engine else if a rule exists, an alert is generated and the event is logged.

4.2.3 Detection Engine:

In this module actual attack identification and detection is carried out by matching each incoming packet with signature database which has been formulated on the basis of previously defined and stored rules. If an attack is suspected, the packet is either dropped or passed depending upon the applicable rules.

4.2.4 Logging and Alerting System:

In this module information received from the detection engines is inspected and based in the rues either generates alert if attack is found and logs packet(s) or both.

4.3 Integration of proposed solution with SNORT

Main issue in Snort is that it lacks the ability to detect attack traffic that don't have any signature match its database. This cause flooding flow based attacks undetected. A rate_filter introduced in Snort version 2.8.5 which aims on DDOS attack detection by filtering packet based on incoming packets from a particular source/detection per unit time. This feature limits the incoming packets based on the source and destination IP/port and the limitation is done by dropping further incoming packets based on already decided unit of time by network administrator. This feature is not very effective and leads to false negatives.

Multiple Sliding window algorithm, as well as the proposed algorithms (refer to Chapter 4 for details) have been integrated with Snort as its dynamic preprocessor.

4.4 Snort Dynamic Preprocessors

Snort dynamic preprocessors which are loadable are developed outside the Snort using snort source code and dynamic libraries to implement MSW correlation and proposed solution.

Snort preprocessors perform multiple operations before the packets are sent to signature database of the detection engine. Preprocessors perform multifarious analysis on packets which is not possible to do inside rule-based detection engine. As already discussed there are multiple preprocessors in Snort that are insufficient for flooding DDoS attacks detection. Following are the major built-in Snort header utilized to develop the dynamic module:

SFSnortPacket header contains SFSnort Packet data structure which is the main source of information from incoming data packet. It is major header file that is used for development of dynamic preprocessor module of Snort.

SF_Dynamic_Preprocessor header contains DynamicPreprocessor which is an important data structure to develop dynamic preprocessor module. It registers the preprocessor, makes it able to start, exit, restart and execute the main processing function. It has the functions for logging, exceptions, fatal errors and debugging information etc.

SF_Packet_info.h is an important header file that is needed for development of said module. It contains information like preprocessor version,name and main packet processing function of the preprocessor.

4.5 Traffic Generation

In this section traffic generation tools are discussed that are used to generate and set up normal and flooding DDoS attack traffic resembling the real-world scenarios. It is worth mentioning that there is a strong lack of attacks representing current and novel DDoS scenarios in the old data sets as DARPA or KDD Cup 1999 Dataset [78][79][80]. The traffic generation mechanism exploits the random packet/source IP generation feature of various attack generation tools. In this process of traffic generation, a single machine is used to generate normal traffic by sending IP packets with varying IP addresses and number of data packets from single source to the destination and by the same method another machine (attack machine) is used to transmit the same to the victim machine but with large amount of changing IP addresses and number of data packets per unit time. Table 4 shows the different traffic generation tools to perform the DDOS attack on a single target.

Table 4.1 Traffic Generation Tools

Traffic Type	**Traffic Generation Tools**
Background Traffic	TCP Replay 4.0.0 , Ostinato 0.8
Attack Traffic	Ostinato 0.8 , Hping3 2.0.0

4.6 Network architecture for Implementation

For implementation of the proposed solution three machines are used which are connected in LAN using a switch and are on same vlan. Machine specification are shown in Table 4.2. Two of the test scenarios are implemented for testing.

Table 4.2 Machine details

Machines	Operating System	Hardware Specification
Detection Engine	Ubuntu, Snort 2.9	Dual Core 2.4 GHZ, 2 GB RAM
Background Traffic Generating Machine	Windows 10 , Ostinato , TCP Replay, Hping 3	Core i3 2.4 GHZ, 6 GB RAM
Attacking Machine / legitimate traffic generation machine	Windows 7, Ostinato 0.8	Corei3 2.4 GHZ, 4 GB RAM

4.6.1 Normal Traffic Test scenario

In normal traffic test case there are three machines used as shown in figure 4.1. First is legitimate traffic machine generating legitimate traffic, second is background traffic generation machine and third machine is snort detection engine. Like attack scenarios which differ in randomness of incoming source IP addresses of the packets and number of packets per unit time, both old and proposed technique have been tested for the degree of false positives. Multiple test cases are used for testing.

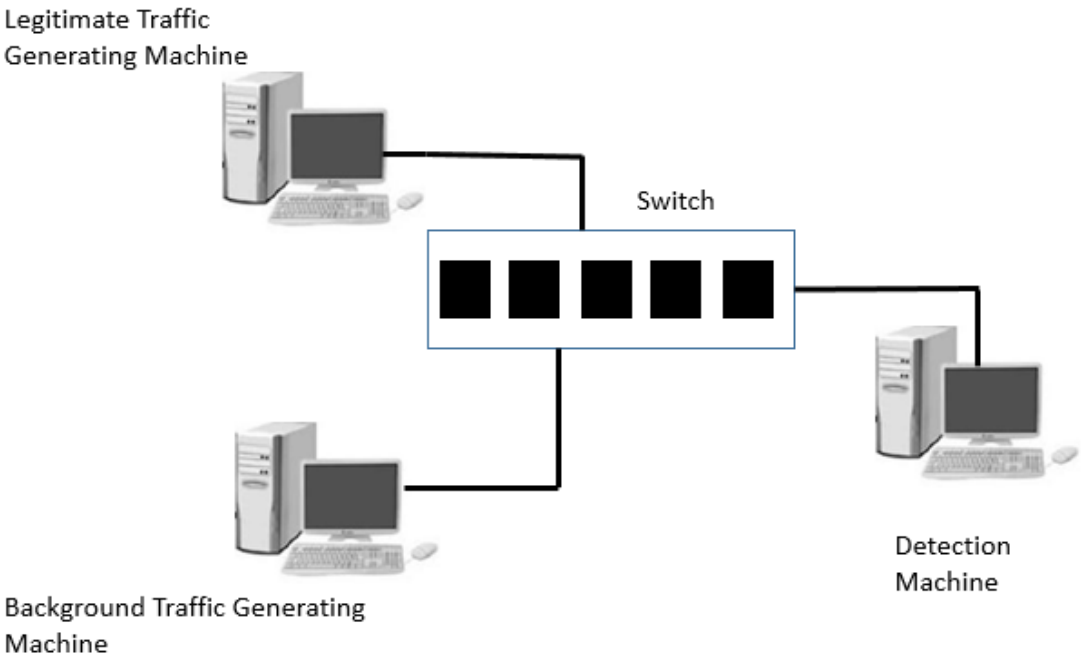

Figure 4.2 Normal Traffic test Scenario

4.6.2 Attack Traffic Test Scenario

In attack traffic test case there are three machines used as shown in figure 4.2. First is attack traffic machine generating attack traffic (DDOS attack), second is background traffic generation machine and third machine is snort detection engine. In attack traffic test scenario number of attack packets are increased in terms of varying IP addresses and number of data packets per unit time. Multiple attack test cases are implemented for testing purposes. The detection capability of both old and proposed technique have been tested under different degree of uniqueness of source IP addresses of the incoming attack packets. Snort detection engine is being targeted for DDOS attack and background traffic is generated as same as in normal traffic test scenario.

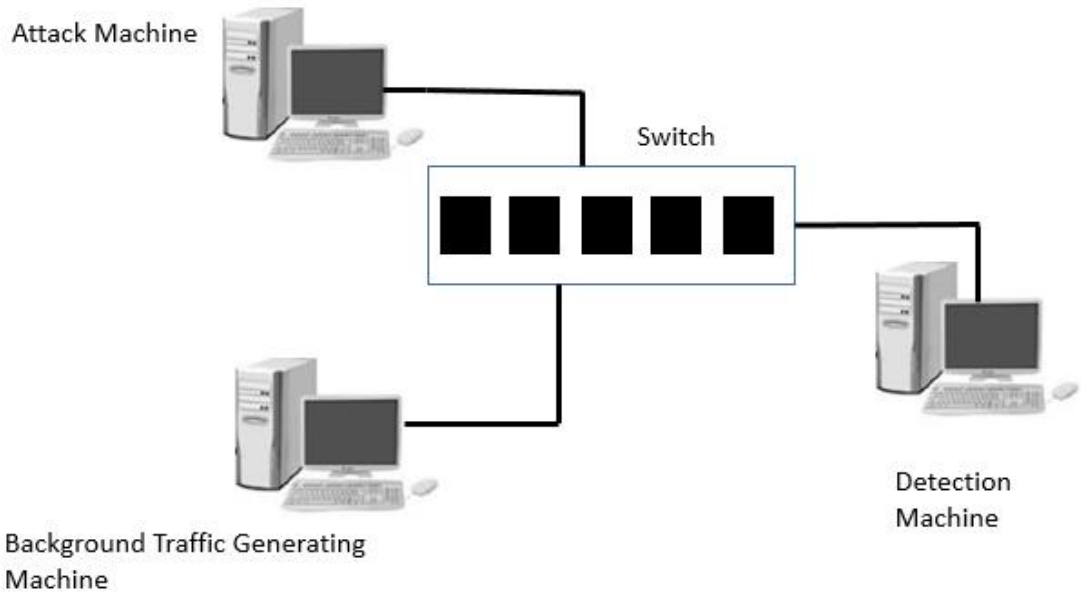

Figure 4.3 Attack Traffic Generation

4.6.3 Implementation Design

As discussed earlier for implementation of the proposed solution three machines are used. Real time hardware resources are used for the purpose as Snort detection capability and results are not effective in virtual environment. Detection engine is implemented using Snort and it is installed on linux based operating system Ubuntu. Snort version 2.9. Dynamic preprocessor for proposed solution and old MSW correlation technique was developed in Snort and implemented on the same machine. All of the traffic for testing is directed towards this machine for detection i.e. normal traffic and background traffic in case of normal traffic test scenario and attack traffic and background traffic in case of attack traffic test scenario. Background traffic generation machine is also a linux based machine using operating system Ubuntu and traffic generation tools i.e. TCP replay and Hping 3. Normal and attack traffic

generation is being carried on windows based operating system using windows 10 and traffic generation tool Ostinato v 0.8.

4.7 Traffic Generation

For the implementation and testing purposes in normal and attack traffic test scenarios separate datasets are defined according to the hardware capability utilized in testing. In both test scenarios IDS is tested for varying amount of IP addresses and number of data packets being sent to the target.

Table 4.3 shows the data traffic in normal test case scenario.

Table 4.3 Normal Traffic Test Scenario Data Traffic

Test Cases	**Packet/sec -Number of IP addresses**	**Packet/sec -Number of IP addresses**	**Packet/sec -Number of IP addresses**	**Background Traffic Packet/sec-Number of IP addresses**
Test case 1	10 p/s - 8 IPs	10 p/s -16 IPS	10 p/s -64 IPS	20 p/s – 8 IPs
Test Case 2	50 p/s - 8 IPs	50 p/s -16 IPS	50 p/s -64 IPS	20 p/s – 8 IPs
Test Case 3	75 p/s - 8 IPs	75 p/s -16 IPS	75 p/s -64 IPS	20 p/s – 8 IPs
Test Case 4	100 p/s-8IPs	100 p/s -16 IPS	100 p/s -64 IPS	20 p/s – 8 IPs

In normal traffic test scenario, number of IP are being increased and same amount of packets per second are tested for every set of IP addresses i.e. incrementing IP addresses. For attack traffic case same method is used but number of IP addresses were increased and number of data packets from unique source are increased as well. In this case as Snort IDS is being hit from large amount of sources (multiple IP addresses) and

as packets amount from each source is also increased resulting in DDOS attack. Table 4.4 shows the attack traffic test scenario data traffic.

Table 4.4 Attack Traffic Test Scenario Data Traffic

Test Cases	**Packet/sec -Number of IP addresses**	**Packet/sec -Number of IP addresses**	**Packet/sec -Number of IP addresses**	**Background Traffic Packet/sec-Number of IP addresses**
Test case 1	500 p/s - 128 IPs	500 p/s - 256 IPs	500 p/s - 512 IPs	20 p/s – 8 IPs
Test Case 2	1000 p/s – 128 IPs	1000 p/s – 256 IPs	1000 p/s - 512 IPs	20 p/s – 8 IPs
Test Case 3	1500 p/s - 128 IPs	1500 p/s – 256 IPs	1500 p/s - 512 IPs	20 p/s – 8 IPs
Test Case 4	2000 p/s - 128 IPs	2000 p/s – 256 IPs	2000 p/s - 512 IPs	20 p/s – 8 IPs

In both cases multiple sets of test results were collected analysis.

4.8 Threshold:

In test cases and environment in which both correlation and mutual information algorithms were tested, the maximum number of packets per second that Snort is able to receive is 3000 and after this it starts to drop the packets.

4.8.1 Threshold for Snort

The "count" in the parameter is to be changed in order to change the threshold. Values of threshold are gauged in a way to find out detection capability in two situations, one with a moderate threshold and the other with a higher value of threshold.

For both the test cases, DDOS detection thresholds for MSW correlation and mutual information were decided on the basis of multiple time data gathered in experimental environment as discussed in section 4.5.

4.8.2 Threshold for Mutual Information Algorithm

The Mutual information values were calculated using the above mentioned test cases It has been found Mutual information values doesn't increase from 1.69 in normal test cases including the peak values hence the threshold for attack was chosen to be 1.69.

4.8.3 Threshold for Correlation and MSW-Correlation Algorithm

The correlation coefficient values of the packets per second has been using same scenarios. It has been found that correlation coefficient values do not fall below 0.003. Hence the threshold for attack is chosen to be 0.0029.

4.9 Conclusion

A simpler and convenient way to achieve DDOS attack is using traffic generator tools available. In two test scenarios network topology and network devices have been arranged physically according to the requirements of different test scenarios.

While keeping the packet per second range steady, variations in the uniqueness of source IP addresses has been tested against both algorithms and for both algorithms. Tests have been done on attack traffic as well as on normal traffic. Based on the scenarios, analysis was with reference to detection capability.

Results and Analysis

5.1 Introduction

This chapter explains the results of the experiments conducted. According to the results, the proposed Mutual Information algorithm successfully identified the attack instances in all the attacks scenarios. The results have been shown below using graphs.

5.2 Results of Test-Bed 1(Design Using Real Systems)

This section explains the results that have been achieved in Test-bed 1 (please refer to Chapter 4 for test-beds details). Results for normal traffic scenarios have been explained in section 5.4.1 and the results of attack scenarios have been given in section 5.4.2.

5.2.1 Results of Normal Traffic Test Scenarios

This section explains the results of normal traffic scenarios belonging to test-bed explained in chapter 4. Please refer to Chapter No. 4 to read details about test-beds and traffic scenarios. The results of Correlation based technique and Mutual Information based technique have been given in sections 5.2.1.1 and 5.2.1.2 respectively.

5.2.1.1 Mutual Information in Normal Traffic Scenario

Mutual information value in normal Traffic scenario is remained between minimum of 0.63 and maximum of 0.698 as shown in Figure 5.1.

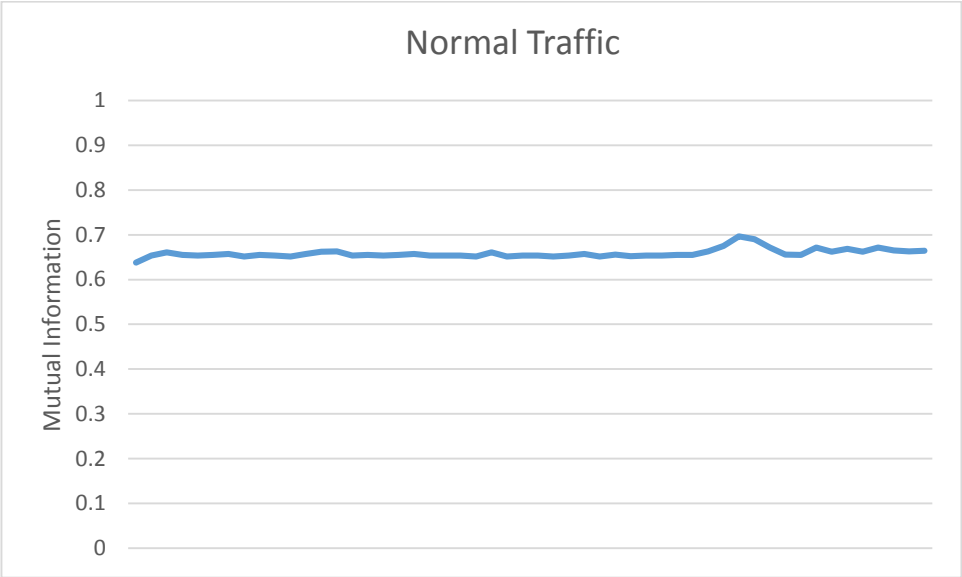

Figure 5.1 Normal Traffic Scenario Result for Mutual Information Algorithm

5.2.1.2 Correlation in Normal Traffic Scenario

Correlation Coefficient value in normal Traffic scenario is remained between minimum of 0.117 and maximum of 0.136 as shown in Figure 5.2.

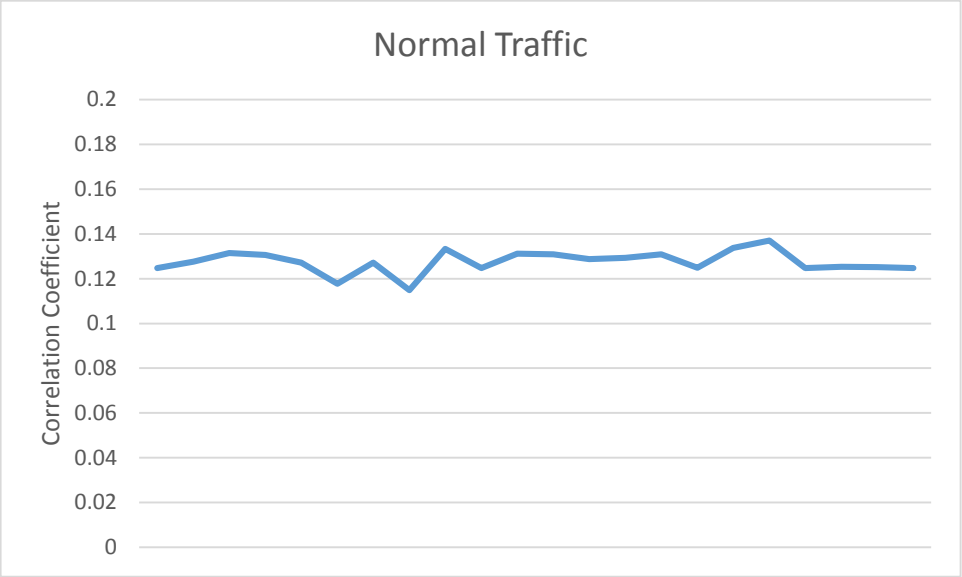

Figure 5.2 Normal Traffic Scenario Result Correlation based Algorithm

5.2.2 Results of Attack Traffic Test Scenarios

This section explains the results of attack traffic scenarios belonging to test-bed explained in chapter 4. Please refer to Chapter No. 4 to read details about test-beds and traffic scenarios. The results of Correlation based technique and Mutual Information based technique have been given in sections 5.2.2.1 and 5.2.2.2 respectively.

5.2.2.1 Mutual Information in Attack Traffic Scenario

Correlation Coefficient value in normal Traffic scenario is remained above 1.5 as shown in Figure 5.3.

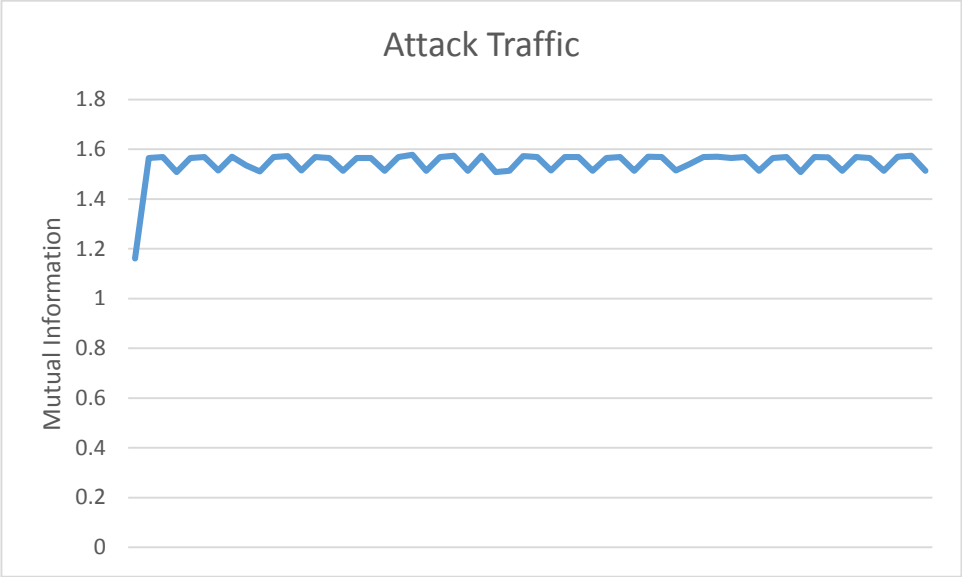

Figure 5.3 Attack Traffic Scenario Result Mutual Information Algorithm

5.2.2.2 Correlation in Attack Traffic Scenario

Correlation Coefficient value in normal Traffic scenario is remained above below 0.029 with exception of some values in range of 0.11 to 0.13 as shown in Figure 5.4.

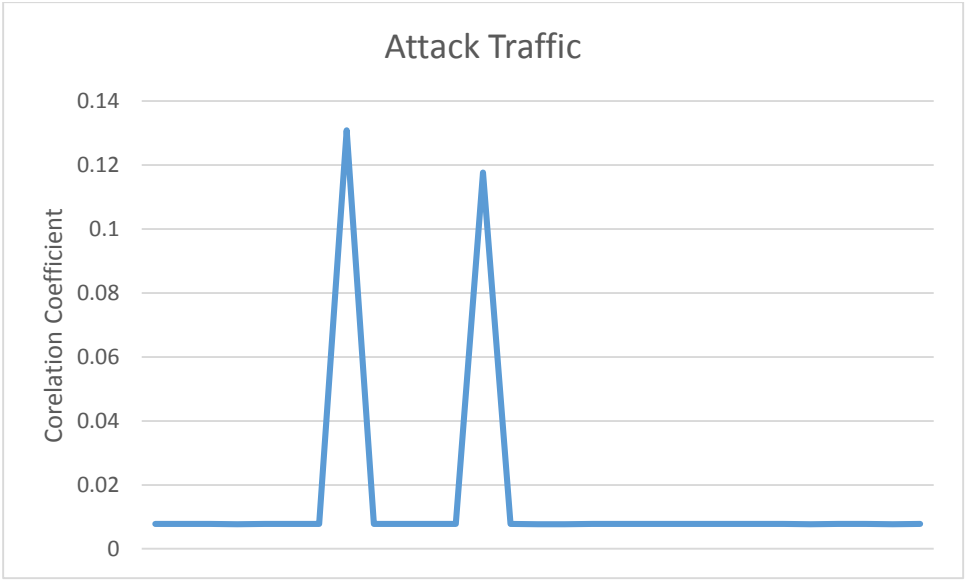

Figure 5.4 Attack Traffic Scenario Result Correlation based Algorithm

5.3 Analysis

The following section gives a detailed analysis of the results of the tested techniques under both attack and normal traffic test scenarios.

5.3.1 Analysis of Results for Correlation based algorithm

Figure 5.2 shows the detection capability of correlation based algorithm in normal traffic test scenario and it shows that the value remained above 0.11. Figure 5.4 shows the detection capability of correlation algorithm in attack traffic test scenario in which value remain below 0.0029 with some exceptions.

To clearly understand the attack and normal traffic test scenario Figure 5.5 shows the detection capability as threshold for the algorithm was set to 0.0029 and during the attack scenario value was remained above 0.0029 which results in false negatives.

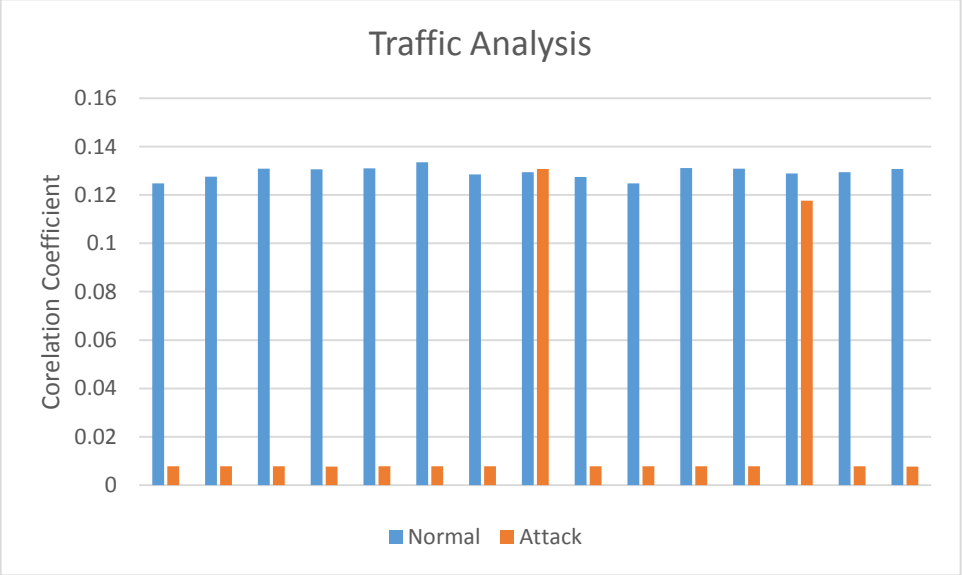

Figure 5.5 Correlation Algorithm Traffic analysis

5.3.2 Analysis of Results for Mutual Information based algorithm

Figure 5.1 shows the detection capability of correlation based algorithm in normal traffic test scenario and it shows that the value remained below 0.69. Figure 5.3 shows the detection capability of correlation algorithm in attack traffic test scenario in which value remain above 1.5 with some exceptions.

To clearly understand the attack and normal traffic test scenario Figure 5.6 shows the detection capability as threshold for the algorithm was set to 0.7.

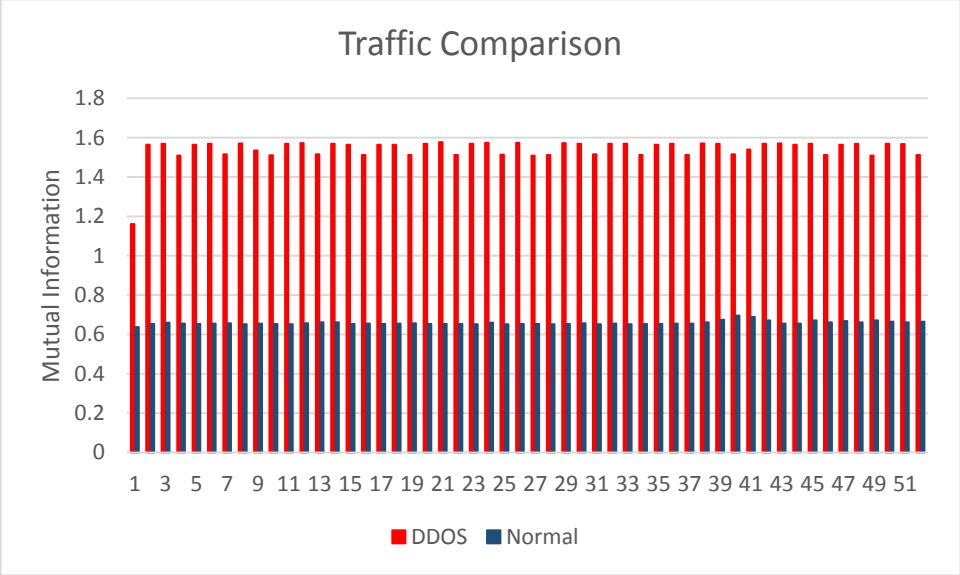

Figure 5.5 Mutual Information Algorithm Traffic analysis

5.4 False Alarms

The analyses of all the algorithms has also been done by counting the false alarms each algorithm gives. As indicated in previous sections, the Mutual Information algorithm technique gives promising results and can distinguish between attack and normal traffic most effectively. Therefore, it gives least false alarms. This has been shown in Figure 5.4 as results shows the false alarms.

Table 5.1 shows the comparison between previous flow based techniques and our proposed solution, based on the results and graphs included in the previous topics.

Table 5.1 Comparison of Flow Based Solutions

Sr. No	Major Flow Based Proposed Scheme	Limitations
1	PCA Based Approaches[48][49]	not practical to be adopted in today's network scenario
2	D-WARD[70]	not memory efficient
3	Temporal Correlation[46]	only for spoofed attack IPs
4	Time series analyses based on HVM[17]	high false positives
5	CPR[50]	insufficient for real time implementation
6	Flow Table[54]	high false alarms, not scalable
7	EWMA [37]	cannot differentiate attack from flash events
8	Chi-Square[73]	not memory efficient
9	HiFIND[58]	high false negatives
10	Change Point Detectors [24][35][36]	high false alarms, complex, not memory efficient
11	NfSen plugin[51]	need to change profile for different attack data sets
12	Traffic Behavior Correlation Analyses[52]	insufficient for real time implementation
13	Proposed Technique	Lesser false positives Lesser CPU intensive ALG

5.4 Conclusion

So far the conducted research in the field of detecting DDoS attack has been a challenging research problem since these attacks must be detected timely and accurately. The main issues with most of the DDoS detection schemes has been that either they are not scalable or not accurate. The primary contribution of this chapter has been the results that are extracted from different attack and normal traffic scenarios.

The results have been analyzed on the basis of detection accuracy and false alarms.

A comparison of the old correlation technique and proposed technique has been given. Results indicate that the rate filter feature of Snort might be useful if the attack is launched from single source IP address, which is generally not the case in flooding DDoS attacks. Practically, in the flooding distributed denial of service attacks, the attack traffic is generated using random source IP addresses. Hence, all the packets in our scenarios bypassed this feature which is the only feature in Snort to defend against flooding DDoS attacks. As indicated by results, the Mutual Information technique gives promising results and can distinguish between attack and normal traffic effectively.

Chapter 6

Conclusion

6.1 Overview

Flooding DDoS attacks are the most difficult attacks to detect timely and accurately. Unfortunately, to address this problem, the rate filtering technique in the present rule-based NIDS is insufficient because the packets sent seem to be legitimate. Also, the packet data does not match with any of the signatures in the NIDS database. Since the sources of flooding DDoS attacks are distributed or have been produced using tools that makes the attack look like coming from several thousand unique sources, it is very easy to bypass rate filters and limitations. The reason is that a very strict and low value of rate filter gives false positives and thus attacks will not be detected accurately. On the other hand, a higher value of rate filter will give false negatives and detect even the legitimate traffic as attack traffic as discussed previously.

6.1 Objectives Achieved

1. The detection techniques used by rule-based NIDS for flooding distributed denial of service attacks have been studied. Detection capability of chosen NIDS, Snort has been observed and analyzed in details with respect to the normal and attack scenarios in terms of false negatives and false positives. It has been seen from the experiments that, by keeping a low value of rate filter, the attacks have been

detected in half of the attack scenarios, but at the same time, the legitimate traffic was detected as attack traffic. While attack detection is the main motivation of rate filter, it should not detect normal traffic as attack. This will interrupt legitimate clients and cause denial of service. In this way, every incoming traffic, whether attack or legitimate, was detected as attack traffic in most of the scenarios. Thus, the detection capability of rate filter technique is found to be severely insufficient.

2. To generate effective results, a sophisticated test bench has been utilized. Both of the algorithms have been analyzed under normal and flooding DDoS attack scenarios and evaluation has been done with respect to their detection accuracy and capability.
3. It has been observed in various recent studies that in order to detect flooding DDoS attacks, flow based techniques give much more promising results than packet based detection techniques. A variety of flow-based DDoS detection algorithms have been studied. Weaknesses in the present flow based DDoS detection techniques have been identified. Analyses Correlating and Mutual Information of traffic flows based on IP addresses.
4. It was found through experimental results that Mutual Information technique is better than Correlation based techniques as it gives lesser false alarms. Hence, this technique was chosen for further improvements that were expected be helpful in giving better results than both of the algorithms.
5. The proposed technique was implemented and integrated with a famous rulebased network intrusion detection system, Snort. The behavior or Snort was evaluated

and then the effects of the integrated algorithm were evaluated to see the impact of the proposed technique.

6.2 Limitations

During the course of the research, few limitations have been observed as follows:

1. The proposed correlation technique is currently using individual feature of packet header, i.e. source IP address.
2. The proposed technique has been tested on a limited number of real world datasets.

6.4 Future Directions

1. An obvious step forward would be to take several features and use Mutual Information to get the relation possible between them. In case of multiple features, weights might be assigned to each feature and weighted Mutual Information might be performed. This step is expected to increase detection capability potentially.
2. The proposed technique can be applied to a wider range of datasets comprising of more complex flooding attack types. This will help to generalize this technique.

6.5 Concluding Remarks

In this information technology based era, flooding DDoS attacks pose serious challenges to digital industries like media, entertainment, technology, financial services security and gaming industries. Rule-based detection despite being the most common method suffers from limitations as it cannot monitor traffic flow and thus cannot detect flooding DDoS attacks efficiently. This thesis has made an attempt to handle this issue. Results have

verified that the proposed technique is effective in detecting not only the attack traffic timely but also in reducing false positive rate. The technique has been integrated with rule-based NIDS, Snort. The proposed technique should be extended to deal with its explained limitations and future directions.

References

[1] "Internet Users in Pakistan", [Online] Available: http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobilereport/

[2] Monowar, Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita, “Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions”, December 2012

[3]"Cyber Security Statistics" [Online] Available: shttp://hackmageddon.com/category/security/cyber-attacks-statistics

[4] "Biggest DDoS Cloudfare", [Online] Available: http://rt.com/news/biggest-ddos-uscloudflare-557/

[5] J. Mirkovic and P. Reiher "A taxonomy of DDoS attack and DDoS defense mechanisms", ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, 2004

[6]"Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 7", Network and System Management (NSM) Data Object Models; International Electrotechnical Commission (IEC): Geneva; Switzerland, 2009

[7]"Introduction to DDoS Attack by NSFOCUS", [Online] Available: en.nsfocus.com/ddos_faq/01-What_is_DDoS_Attack-EN.html

[8] "Dangerous DDoS (Distributed Denial of Service) on the rise" , [Online] Available:

http://resources.infosecinstitute.com/dangerous-ddos-distributed-denial-of-service-onthe-rise/

[9] "Layer seven DDoS Attacks", [Online] Available: http://resources.infosecinstitute.com/layer-seven-ddos-attacks/

[10] "Q1 2014 Global Attack Report" [Online] Available : http://www.prolexic.com"

[11] "Akamai Publishes Prolexic Q1 2014 Global DDoS Attack Report" [Online] Available: http://www.akamai.com/html/ about/press/ releases /2014/press041714.html

[12] "DDoS Report 2014" [Online] Available : http://www.prolexic.com/knowledgecenter-ddos-attack-report-2014-q1.html

[13] A. Saboor, M. Akhlaq, B.Aslam, "Experimental evaluation of Rule-based NIDS against DDoS attacks under different hardware configurations", In Proceedings of 2nd National Conference on Information Assurance (2013)

[14] H. Alaidaros, M. Mahmuddin and A. Al Mazari , “An Overview Of Flow-Based And Packet-Based Intrusion Detection Performance In High Speed Networks”, in Proceedings of the International Arab Conference on Information Technology (ACIT 2011), Riyadh, 2011

[15] A. Sperotto, “An Overview of IP Flow-Based Intrusion Detection,” IEEE Communications Surveys Tutorials, vol. 12, no. 3, 2010

[16] J. Vykopal, "Flow-based Brute-force Attack Detection in Large and High-speed Networks", Ph.D. dissertation, Masaryk University, 2013

[17] A. Sperotto, "Flow-based intrusion detection," Ph.D. dissertation, University of Twente, October 2010

[18] “Rule-based NIDS” [Online]. Available: www.Rule-based NIDS.org

[19] "Network Intrusion Detection and Mitigation against Denial of Service Attack" , [Online]. Available: www.cis.upenn.edu/~lindong/paper/wpe2.pdf(2013)

[20] P. Barford and D. Plonka, "Characteristics of Network Traffic Flow Anomalies" , In Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, pages 69–73. ACM, 2001

[21] "DDoS protection flow detection overview", [Online]. Available: http://www.juniper.net/techpubs/en_US/junos13.3/topics/concept/subscribermanagement-scfd-overview.html

[22] "The Bro Network Security Monitor ", [Online]. Available: www.bro.org/

[23] Gavrilis, D. and Dermatas, "Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features", Computer Networks and ISDN Systems, 48, 235–245,2005

[24] J. Li, Y. Liu, and L. Gu, “DDoS Attack Detection Based On Neural Network,” Proc. of 2nd Intl’ Symposium On Aware Computing (ISAC), IEEE, pp. 196-199, November 2010

[25] R. Karimazad and A. Faraahi, "An anomaly-based method for DDoS attacks detection using RBF neural networks" In proceedings of the International Conference on Network and Electronics Engineering, Singapore, pp. 44–48. IACSIT Press, 2011

[26] Kumar , P. A. R. and Selvakumar, S. (2011) Distributed denial of service attack detection using an ensemble of neural classifier. Computer Communication, 34, 1328–1341

[27] P. Agarwal, B. Gupta, S. Jain, and M. Pattanshetti, “Estimating Strength of a DDoS

Attack in Real Time Using ANN Based Scheme," Communications in Computer and Information Science, Springer, 2011, vol. 157, part 6, pp. 301-310.

[28] B. Gupta, R. Joshi, M. Misra, A. Jain, S. Juyal, R. Prabhakar, and A. Singh, "Predicting Number of Zombies in a DDoS Attack Using ANN Based Scheme," Communications in Computer and Information Science, Springer, 2011, vol. 147, part 1, pp. 117-122.

[29] H. Xu, B. Chen, F. Yang, and F. Liu, "Fast Algorithm of Evolutional Learning Neural Network," Proc. of Int'l Conf. On Intelligent Systems Design and Engineering Application (ISDEA), IEEE, pp. 262-265, January 2012.

[30] M. Aamir und A. Zaidi, "DDoS Attack and Defense: Review of Some Traditional and Current Techniques". In proceedings of CoRR abs, 1401.6317, 2014.

[31] F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," CERT Coordination Center, Special Report: CMU/SEI-2002-SR-009, November 2002

[32] K. Kumar, L. Sangal, and A. Bhandari, "Traceback Techniques Against DDoS Attacks: A Comprehensive Review," In proceedings of Conference On Computer and Communication Technology (ICCCT), IEEE, pp. 491-498, September 2011

[33] K. Subhashini, and G. Subbalakshmi, "Tracing Sources of DDoS Attacks in IP Networks Using Machine Learning Automatic Defence System," International Journal of Electronics Communication and Computer Engineering, vol. 3, issue 1, pp. 164-169, January 2012

[34] H. Beitollahi, and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," Computer Communications, Elsevier, vol. 35, issue

11, pp. 1312-1332, June 2012.

[35] A. Siris and F. Papagalou, “Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks,” in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM’04), vol. 4, Dallas, USA, pp. 2050–2054, 2004.

[36] H. Wang, D. Zhang, and G. Shin, “SYN-dog: Sniffing SYN Flooding Sources,” in Proceedings of the 22th International Conference on Distributed Computing Systems. Washington, DC, USA: IEEE Computer Society, pp. 421–429, 2002.

[37] N. Ye, S. Vilbert, and Q. Chen, "Computer intrusion detection through EWMA for auto correlated and uncorrelated data," In proceedings of *EEE* Trans. Rel., vol. 52, no. 1, pp. 75–82, March 2003.

[38] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing Network-Wide Traffic Anomalies,” in Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications(SIGCOMM’04), pp. 219–230, 2004

[39] L. Huang, X. Nguyen, M. Garofalakis, and M. Hellerstein, “Communication-Efficient Online Detection of Network-Wide Anomalies,” in IEEE Conference on Computer Communications (INFOCOM’ 07) , pp. 134–142, 2007

[40] N. L. D. Khoa, T. Babaie, S. Chawla, and Z. Zaidi, “Network Anomaly Detection Using a Commute Distance Based Approach,” in International Conference on Data Mining Workshops (ICDW’10), pp. 943–950, 2010

[41] H. Ringberg, A. Soule, J. Rexford, and C. Diot, “Sensitivity of PCA for Traffic Anomaly Detection,” in Proceedings of the ACM SIGMETRICS’ 07, pp. 109–120, 2007

[42] 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

[43] Wu, Y. C., Tseng, H. R., Yang, W., and Jan, R. H., "DDoS detection and trace-back with decision tree and grey relational analysis", International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136, 2011

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

[45] H. Rahmani, N. Sahli and F. Kammoun, "Joint entropy analysis model for DDoS attack detection" In proceedings of the 5th International Conference on Information Assurance and Security, 2009.

[46] K. Lu, D. Wu, and J. Fan, “Robust and efficient detection of DDoS attacks for largescale internet,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 51, no. 18, pp. 5036–5056, Dec 2007.

[47] M. Handley, “Internet architecture WG: DoS-resistant internet subgroup report,” Technical Report, 2005.

[48] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing network-wide traffic anomalies,” in proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications, Portland, Oregon, USA, pp. 219–230, 2005

[49] “Mining anomalies using traffic feature distributions,” in proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications, Philadelphia, Pennsylvania, USA, pp. 217–228, 2005

[50] C. Zhang, Z. Cai, Chen, X. Luo and J. Yin, "Flow level detection and filtering of lowrate DDoS" Computer Networks, 56, 3417–3431, 2012

[51] L. Hellemons, L. Hendriks, R. Hofstede, A. Sperotto, R. Sadre, A. Pras, "SSHCure: A Flow-Based SSH Intrusion Detection System. In proceedings of AIMS 2012. LNCS, vol. 7279, pp. 86–97. Springer, Heidelberg, 2012

[52] D. Cabrera, "Proactive detection of distributed denial of service attacks using MIB traffic variables-a feasibility study," pp. 609-622, 2001

[53] 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.

[54] A. Sanmorino, S. Yazid, “DDoS Attack Detection Method and Mitigation Using Pattern of the Flow”, IEEE International Conference of Information and Communication Technology, 2013

[55] Z. Wang, X. Wang , "DDoS attack detection algorithm based on the correlation of IP address analysis" In Proceedings of the 2011 International Conference on Electrical and Control Engineering (ICECE). Yichang, 2011

[56] J. Jung et al. Fast portscan detection using sequential hypothesis testing. In Proc. of the IEEE Symposium on Security and Privacy, 2004.

[57] "Deterlab, based on Emulab", [Online] Available: http://www.deterlab.net/

[58] Y. Gao, Z. Li, Y. Chen, "A DoS Resilient Flow-level Intrusion Detection Approach for High-speed Networks", 2006

[59] J. Cheng, J. Liu, "DDoS Attack Detection Algorithm Using IP Address Features" In Proceedings of FAW 2009. LNCS. Springer, Heidelberg (2009)

[60] J. Vykopal, "Flow-based Brute-force Attack Detection in Large and High-speed Networks", Ph.D. dissertation, Masaryk University, 2013

[61] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS). NIST", Recommendations of the National Institute of Standards and Technology. Retrieved online December 26, 2009"

[62] B. Claise, "Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational)", October 2004

[63] D. Kumar, Dr C. Guru Rao, Dr M. Singh, Dr Satyanarayana, "A Survey on Defense Mechanisms countering DDoS Attacks in the Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2013

[64] H. Monowar, J. Bhuyan, D. Kashyap, K. Bhattacharyya and K. Kalita, “Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions”, December 2012

[65] O. Salem, A. Makke, J. Tajer, and A. Mehaoua, "Flooding Attacks Detection in Traffic of Backbone Networks," in LCN, 2011, pp. 441-449.

[66] E. Ahmed, A. Clark, and G. Mohay, "A Novel Sliding Window Based Change Detection Algorithm for Asymmetric Traffic", In NPC 2008 IFIP International Conference on Network and Parallel Computing, 2008, pages 168–175. IEEE, 2008.

[67] E. Ahmed, A. Clark, and G. Mohay, "Effective Change Detection in Large Repositories of Unsolicited Traffic", In Proceedings of the Fourth International Conference on Internet Monitoring and Protection, May 2009.

[68] H. Takada and U. Hofmann. "Application and Analyses of Cumulative Sum to Detect Highly Distributed Denial of Service Attacks using Different Attack Traffic patterns, April 2004", [Online] Available : http://www.ist-intermon.org/dissemination/newsletter7.pdf

[69] H. Liu and S. Kim, “Real-Time Detection of Stealthy DDoS Attacks Using Time-Series Decomposition”, in Proceedings of IEEE International Conference on Communications (ICC), 2010

[70] J. Mirkoviac, G. Prier, and P. Reiher, "Attacking DDoS at the source. Proceedings of the 10th IEEE International Conference on Network Protocols", Paris, France, 12-15 November, pp. 1092–1648. IEEE CS, 2002

[71] L. Chen,, "A new detection method for distributed denial-of-service attack traffic based on statistical test", Journal of Universal Computer Science, 15, 488–504, 2009

[72] D. Kale, IIProf. V. Bhosale, " Scrutiny of DDoS Attacks Defense Mechanisms", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2 Issue 1, 2014

[73] 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, volume 1, pages 303–314. IEEE., 2003.

[74] J. Buchanan, J. Graves, R. Macfarlane “A Methodology to Evaluate Rate-Based Intrusion Prevention System against Distributed Denial-of-Service”, In Cyberforensics 2011.

[75] " Downloads for Snort IDS",[Online] Available: https://www.snort.org/downloads

[76] M. Akhlaq, F.Alserhani, I.U.Awan, J.Mellor, A.J.Cullen,P. Mirchandani, "Virtualization Efficacy for Network Intrusion Detection Systems in High-speed Networks" in Weerasinghe, D. (ed.) IS&DF, vol. 41, pp. 26–41. Springer, Heidelberg, 2010

[77] F.Alserhani, M.Akhlaq, I.Awan, A.Cullen, J.Mellor, P.Mirchandani,"Evaluating Intrusion Detection Systems in High Speed Networks" In proceedings of 5th International Conference of Information Assurance and Security (IAS 2009). IEEE Computer Society, Los Alamitos, 2009

[78] "The UCI KDD Archive University of California, Department of Information and Computer Science", [Online] Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html,

[79] J. McHugh, "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory", ACM Transactions on Information and System Security (TISSEC), 3(4):262–294, 2000.

[80] M. Tavallaee, E. Bagheri, W. Lu and A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set", In Proceedings of the 2009 IEEE Symposium Computational Intelligence for Security and Defense Applications (CISDA 09)", IEEE Computer Society, 2009

[81] "Layer 7 DDoS Attacks, OWASP, 2010", [Online]. Available: https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf

[82] "LOIC Project, SourceForge", [Online]. Available: sourceforge.net/projects/loic/

[83] "Ddos: Survey of traceback methods," A.John and T. Sivakumar, in International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[84] "The DETER Testbed: Overview",[Online], Available: *w*ww.isi.edu/deter/docs/testbed.overview.pdf

[85] "Using the Deter Test-bed by Ted Faber, 24 January 2011",[Online] Available: www.isi.edu/deter/docs/DETER_Tutorial-TF-Jan2011.pdf

[86] "tcpreplay". [Online]. Available: tcpreplay.synfin.net/wiki/Download

[87] "hping3". [Online]. Available*:* www.hping.org/hping3.html

[88] "Ostinato". [Online]. Available: code.google.com/p/ostinato/

[89] "Wireshark" [Online]. Available: https://www.wireshark.org/download.html

[90] "Cisco Catalyst 2960 Series Switches". [Online]. Available: http://www.cisco.com/en/US/products/ps6406/index.html

[91] Cearns, "Design of An Autonomous Anti-DDoS Network (A2D2),", Thesis, University of Western Ontario, London, Canada, 2002

[92] C. Akyazi and A. S. E. Uyar, “Distributed Intrusion Detection using Mobile Agents against DDoS Attacks,” in Proceedings of 23rd International Symposium on Computer and Information Sciences (ISCIS ’08), Istanbul, 2008, pp. 1-6

[93] Rik Busschers, “Effectiveness of Defense Methods Against DDoS Attacks by Anonymous”, University of Twente, 2010

[94] "Snort Manual: Rate Filtering", [Online] Available: manual.snort.org/node19.html

[95] Prahlad Fogla Giorgio Giacinto Wenke Lee Roberto Perdisci, Da-vide Ariu, Mcpad: A multiple classifier system for accurate payload-based anomaly detection, Computer Networks 53 (2009), 864-881

[96] K. Wang and S. Stolfo. Anomalous payload-based worm detection and signature generation. In Recent Advances in Intrusion Detection (RAID), 2005

[97]"Prolexic DDoS Attack Report 2013", [Online], Available: http://www.prolexic.com/news-events-pr-increasing-size-of-individual-ddos-attacks-20-gbps-is-the-new-norm-2012-q3.html

[98] "Cyber Attack Statistics 2013 by HackGeddon", [Online]. Available: http://hackmageddon.com/2013-cyber-attacks-statistics/