

**A BEHAVIOR BASED ALGORITHM TO DETECT
SPAM BOTS**

BY

MOHAMMED FADHIL ZAMIL

**Thesis submitted in partial fulfillment of the
requirements for the degree of
Master of Science**

June 2009

DECLARATION

Name: Mohammed Fadhil Zamil

Matric No: Pcom0061/08

Faculty: Computer Science

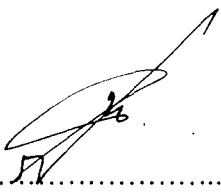
Thesis Title: A Behavior Based Algorithm to Detect Spam Bots

I hereby declare that this thesis in I have submitted to School of Computer Science on 22.16.1.2009..... is my own work. I have stated all references used for the completion of my thesis.


I agree to prepare electronic copies of the said thesis to the external examiner or internal examiner for the determination of amount of words used or to check on plagiarism should a request be made.

I make this declaration with the believe that what is stated in this declaration is true and the thesis as forwarded is free from plagiarism as provided under Rule 6 of the Universities and University Colleges (Amendment) Act 2008, University Science Malaysia Rules (Student Discipline) 1999.

I conscientiously believe and agree that the University can take disciplinary actions against me under Rule 48 of the Act should my thesis be found to be the work or ideas of other persons.

Students Signature: 

Date: 22.16.1.2009.....

Acknowledgement of receipt by: 

Date: 06.07.2009

ACKNOWLEDGMENTS

First of all, I would like to thank the Almighty Allah, the most merciful, the most beneficent for giving me the opportunity to do my post graduate in the School of Computer Sciences, Universiti Sains Malaysia.

I would also like to express my unquantifiable heartfelt gratitude and special regards to my parents and my brother Safaa and the most beautiful smiles of my life; Mustafa and Mufaq who are always there for me. The successful completion of my work is the fruit of their sacrifices, encouragement and devotion. In fact words are not enough; thank you very much.

I wish to record my deep sense of gratitude and appreciations to my supervisor Professor Dr.Sureswaran Ramadass for his expert guidance and support throughout my research tenure.

My acknowledgment goes also to my coordinator Dr. Shahida Sulaiman for her patience and wisdom that made things immensely easier for me and lead to the success of my research.

Last but not least, I have been extremely lucky to have support, encouragement, and inspiration from many people; without them, this work would not have been possible. Here, I would also like to extend my sincere appreciations to my friends Ahmed Ali, Salah, Samer, Ali, Adel Nathem, Awsan Hassan, Bilal and all NAv6 members, as they generously gave me very good pieces of advice and assisted me in my research work.

TABLE OF CONTENTS

DECLARATION	ii
ACKNOWLEDGMENTS	iii
LIST OF TABLES	vii
LIST OF FIGURES	viii
LIST OF SYMBOL AND ABBREVIATIONS	ix
ABSTRAK	xi
ABSTRACT	xiii

CHAPTER 1: INTRODUCTION

1.1 Overview	1
1.1.1 Botnet	2
1.1.2 Botnet Activities	2
1.1.3 Spam Botnet	3
1.2 Problem statement	4
1.3 Motivations	4
1.4 Objectives	5
1.5 Scope of the Study	5
1.6 Proposed Method	6
1.7 Research Methodology	6
1.7.1 Evaluation and Verification	7
1.8 Outline of thesis	8

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction	9
2.2 E-mail System	9
2.2.1 E-mail Sending Scenario.....	9
2.2.2 Domain Name System Protocol (DNS)	11
2.2.3 Simple Mail Transfer Protocol (SMTP).....	12
2.3 Services Scanner attacks	13
2.3.1 Scanning Techniques	13
2.4 Existing Work on Spam Detection	15
2.4.1 White list Filter.....	16
2.4.2 Black List Filter	16
2.4.3 Grey list filter	17
2.4.4 Signature-based Spam Detection.....	18
2.4.5 Behavior-based Spam Detection	20
2.5 Critical analysis	26
2.6 Chapter Summary	27

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction	29
3.2 Abnormal Behaviours in Preparing and Sending Spams.....	29
3.3 Proposed System Framework.....	31
2.5 Calculating the Host Behaviour Relation (Gower's Coefficient)	43
2.6 The Chapter Summary	43

CHAPTER 4: IMPLEMENTATION AND RESULTS

- 4.1 Introduction..... 45
- 4.2 Implementation..... 45
 - 4.2.1 System Tools 45
 - 4.2.2 Database Structure 46
- 4.3 Performance Test of BSD System 47
 - 4.3.1 Hardware Resources of the Experiment..... 47
 - 4.3.2 BSD Position in Network..... 49
 - 4.3.3 Experiment Goals 49
 - 4.3.4 Experiment Scenario 50
 - 4.3.5 The Spam Bot Simulator’s Objectives and Characteristics 51
- 4.4 Performance Test Results..... 52
- 4.5 Goals Achieved by the Experiment 57
- 4.6 BSD System Evaluation..... 57
 - 4.6.1 Detection Rate Evaluation..... 57
 - 4.6.2 False Negative Evaluation..... 58
 - 4.6.3 False Positive Evaluation 59
- 4.7 The Chapter Summary 60

CHAPTER 5: CONCLUSION AND FUTURE WORK

- 5.1 Conclusions 62
- 5.2 Future work 64

REFERENCES 65

APPENDX (A) 69

LIST OF TABLES

Table 2.1: Log of the Security Detecting System (Jian et al., 2007)	22
Table 2.2 : Results of the Jian et al's System (Jian et al., 2007).....	23
Table 2.3: Existing Work and Techniques	27
Table 3.1: System Attributes Method and Goals	44
Table 4.1: Packets Table Structure.....	46
Table 4.2: Abnormal Behaviors Table Structure	47
Table 4.3: BSD Host Hardware and Software Characteristics	49
Table 4.4: Behavior Table after Analyzing the Captured Traffic.....	52
Table 4.5: Proximity Matrix (Gower coefficient).....	54
Table 4.6: List of Similar Objects (Dissimilarity Threshold = 0.5).....	56
Table 4.7: False Negative Case Host (3)	58
Table 4.8: False Positive Case Host (6) Behaving.....	59

LIST OF FIGURES

Figure 1.1: The Main Phases of Proposed Framework	7
Figure 2.1: E-mails Sending Process	9
Figure 2.2: How to Resolve MX Records (Microsoft, 2005a)	11
Figure 2.3: DNS Query Processes (Microsoft, 2005b)	12
Figure 2.4: How DNSBL Works (TrendMicro, 2008a)	16
Figure 2.5: The Differences Between Black, White, and Grey Filters (Harris, 2003)	18
Figure 2.6:Kaspersky Anti-Spam Project Structure (kaspersky, 2008)	19
Figure 2.7: Sandford system structure (Sandford et al., 2006)	24
Figure 3.1: Behavioural-based Spamming Detector (BSD) System Framework	32
Figure 3.2: Capturing and Decoding Stage Process	33
Figure 3.3: Monitoring and Recording Any Suspicion Packets	34
Figure 3.4: Monitoring SMTP packets	35
Figure 3.5: The ideal case of establishing SMTP session	35
Figure 3.6: How to Extract the SMTP Message Code	36
Figure 3.7: Closed Port Case	38
Figure 3.8: Scanning RST Flagged Packet	38
Figure 3.9: Detecting scanning attempts in network	39
Figure 3.10: Open Relay and SMTP Server Priority Tests	40
Figure 3.11: Connecting To Multiple Mail Servers Test	41
Figure 3.12: Rapid Connections Made T_n	41
Figure 4.1: Database Operations in BSD System	47
Figure 4.2: Experiment Network Structure	48
Figure 4.3: Spam Bot Simulator Screenshot	51
Figure 4.4: How Hosts Behave on the Network	55

LIST OF SYMBOLS AND ABBREVIATIONS

ACK	Acknowledgement Packet
BSD	Behavioral-based Spamming Detector
DB	Database
DDoS	Distributed Denial of Service
DNS	Domain Name System
E-mail	Electronic mail
FIN	Finish
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
IM	Instant Message
MAC	Media Access Control
MDA	Mail Delivery Agent
MTA	Mail Transfer Agent
MX	Mail Exchange Server
P2P	Peer to Peer
QoS	Quality of Service
RCP	Rich Client Platform
RST	Reset
SMTP	Simple Mail Transfer Protocol
SYN	Synchronous
TCP	Transport Control Protocol

UDP

User Datagram Protocol

Σ

Summation

PERLAKUAN BERDASARKAN ALGORITMA UNTUK MENGESAN SPAM BOTS

ABSTRAK

Satu daripada masalah utama dan serius dalam rangkaian pada masa ini ialah Spam. Spam merujuk kepada penyalahgunaan sistem mesej elektronik untuk menghantar mesej pukal yang tidak diminta secara rawak. Mengikut kajian terdahulu, Botnet didapati merupakan sumber utama spam. Botnet merujuk kepada satu kumpulan perisian yang dikenali sebagai bot. Fungsi bot ini adalah untuk menjalankan beberapa komputer yang terjejas secara autonomi dan automatik. Penspaman menyebabkan penggunaan haram sumber rangkaian secara amnya dan sistem mel secara khususnya. Objektif kajian ini adalah untuk mengesan sumber spam dalam rangkaian dengan cara mengesan perlakuan tidak normal yang terhasil daripada aktiviti penspaman. Ini dilakukan dengan menggunakan suatu algoritma yang sesuai yang dapat mengenal pasti perlakuan tidak normal yang berkaitan dengan aktiviti spam. Pengesanan Penspaman berasaskan Perlakuan (*Behavioral-based Spamming Detector*, BSD) menggabungkan beberapa perlakuan bot spam pada peringkat yang berlainan termasuk perlakuan penyediaan sumber spam iaitu sebelum bermulanya sesi spam apabila penspam sedang mencari suatu perkhidmatan SMTP geganti terbuka bagi menghantar e-mel. Turut diselidiki ialah perlakuan penspam ketika dihubungkan dengan pelayan mel. Berdasarkan kaedah kajian yang dicadangkan, trafik rangkaian dipantau untuk mengesan aktiviti yang berniat jahat yang dilakukan secara berkumpulan dan setiap kumpulan melakukan aktiviti yang sama. Hubungan antara perlakuan hos yang mencetuskan rasa sangsi adalah digunakan untuk mengesan sama ada terdapat sebarang bot spam atau Botnet dalam

rangkaian. Dapatan kajian ini menunjukkan bahawa kaedah yang dicadangkan mempunyai kadar pengesanan sebanyak 83.3% dengan satu kes positif palsu dan satu kes negatif palsu.

A BEHAVIOR BASED ALGORITHM TO DETECT SPAM BOTS

ABSTRACT

One of the major and recent serious problems on the networks is Spam. Spam refers to the abuse of electronic messaging system by sending unrequested bulk messages randomly. According to the previous researches Botnets are the main sources of spams. Botnet refers to a group of software called bots. The function of these bots is to run on several compromised computers autonomously and automatically. Spamming causes illegal consuming of network resources in general and mail system in particular. The objective of this research is to detect the source of spam on the network by detecting the abnormal behaviors that reflect spamming activities. This is performed by using a suitable algorithm that can identify the abnormal behaviors that related to the spam activity. Behavioral-based Spamming Detector (BSD) combines several behaviors of the spam bots at different stages including the behavior of spam resources preparing which is before the spam session when the spammers search for an open relay SMTP service to send e-mails through, and the behavior of spammers while connecting to the mail server. The proposed research method monitors the network traffic to detect malicious activities which are performed in groups and each group does the same activity. The relationship between the host behaviors that trigger suspicion is used to find out if there are any Spam bots or Botnet members on the network. The results due to experiments showed that the proposed method had 83.3% as detection rate with two false positive and negative cases.

CHAPTER 1

INTRODUCTION

1.1 Overview

The rapid increase of computer network techniques and the high quality of services have made computer connection from one PC to another much faster and easier through the Internet cloud. These features have given networks the reliability to take the first position among all other kinds of communication. Such facilities have allowed connected computers, smart mobiles and laptops to share and transmit data and e-mails more easily and instantly. Thus, security has become increasingly important and necessary due to the dependency on the world-wide spread of network computers and the huge number of users.

The e-mail system is a digital online communication service that sends messages to recipient(s). The task of sending an e-mail can be performed by any computer connected to a network, such as the Internet network. There are several challenges faced by the e-mail systems (Qiong *et al.*, 2007); for example, the increase of harmful techniques has forced e-mail users to search for the higher degree of safety and privacy to ensure the security of the transmitted information. This is due to the recent spread of viruses, hackers, malwares, worms, and Botnets.

Spam is one of these challenges; it abuses the electronic messaging system by sending a huge amount of unrequested bulk messages randomly. According to (Sauer, 2005) who referred to MacAfee website titled "Security Insight on the Web", the author stated that "Most available statistics agree that at least 80 percent or more of all E-mail messages are spam". The reason behind this high percentage is

due to the armies of the harmful bots that are controlled by a botmaster. The botmaster sends commands to these compromised computers called 'zombies' on a network to perform several malicious attacks.

1.1.1 Botnet

Botnets refer to a group of software called 'bots' or 'rebots'. The function of these bots is to run on several computers autonomously and automatically (Zhaosheng *et al.*, 2008). This kind of software usually works at the end-user system that has been infected. Once these bots are installed, they send an identification message to the botmaster. The botmaster can start any command and control session by using these infected computers that are called 'zombies'. The botmaster performs illegal attacks on all these zombies.

Bots work under shadow to avoid being detected by an antivirus or observed by a user. Bots software has the ability to disable the antivirus effect by producing an anti antivirus (Sauver, 2005). The best time for the bots to start performing their activities is during the idle period of the host computer. This happens especially when the bots sense the low CPU utilization, hence they start to profiteer the infected host resources to do their desired activities.

1.1.2 Botnet Activities

Botnets can be classified according to their activities (Xiang and Li, 2006, Linfeng and Yong, 2008) Botnets have several activities such as Distributed Denial of service (DDos), Click Fraud and Spam. This research is focuses on spam activity.

1.1.3 Spam Botnet

The Botnet's strength comes from the number of zombies that can be controlled. "Bots" act in a similar way as worms in their propagation attempts between the computers in a network. The increasing number of zombie machines strengthens the Botnet capabilities. A computer may receive unwanted e-mails which usually contain commercial materials, adult materials and website advertisements that might be attached with harmful software like malware, viruses, and bots. This software is used to propagate between networked computers by performing discrete or multiple actions such as spamming (Zhaosheng *et al.*, 2008).

E-mail services are widely used and trusted by a huge number of users. This is because e-mail services are either cheap or free of charge and reliable. Recently, mobile technology has started utilizing e-mailing and instant messaging (IM) services because these features have huge popularity. Therefore, using e-mails has become the best option to propagate and spread spam of (the unwanted e-mails) to the users' inbox.

This research attempts to detect spam Botnet activities that could lead to Botnet detection. Detecting the abnormal behaviour produced by the spam activities gives a high rate of suspicion on the existence of bots. Spamming techniques often change to prevent detection through defence software. The current techniques of the antivirus/anti-spam can detect spam by screening the content of e-mails which are widely used nowadays to mitigate spam e-mails (Miao *et al.*, 2008). The recent spamming techniques and the method of how the e-mail system works will be reviewed in more detail in Chapter 2.

1.2 Problem Statement

This section is to conclude the previous sections discussed earlier. Consequently, Spam can be classified into two perspectives: end-user and QoS technical networks. Accordingly, the problem can be summarized as follows:

- (i) **The end-user perspective:** Spam refers to unwanted e-mails that come through advertising agents for commercial reasons or from hackers. The spam could be a carrier of harmful software (bots, worms and malware).
- (ii) **The network level perspective:** Spam increases the load on the networks and reduces the Quality of Service (QoS) of the network in general and e-mail service in particular, by generating a number of unwanted traffic.

Based on the problem that is mentioned above, the current research proposes to detect the activates of spam bots and the network traffic related to them.

1.3 Motivations

Spam is a problem that began a long time ago. Many studies and researches have dealt with this problem, but it requires further investigation as they mitigated it, but did not prevent it. In 2004, Bill Gates predicted that “spam will be gone in two years” (Weber, 2004). This raises the question of whether the new techniques can help to make communications safer, easier and faster. As long as this development goes on, spammers and hackers will continue to employ certain techniques to increase spamming. Spam is still increasing that 80% of the e-mails are spam (Sandford *et al.*, 2006). This shows that the problem is still growing.

1.4 Objectives

The main goal of this research is to propose a spam Botnet detection framework which is capable of identifying spam Botnet based on the malicious behaviours of the Botnet activities. The main objectives of this research are listed below:

- (i) To propose a method for identifying unwanted traffic related to spam Botnet.
- (ii) To propose and develop generic procedures that detect compromised hosts involved in Botnet spamming activities.
- (iii) To evaluate the proposed method based on the detection accuracy.

1.5 Scope of the Study

This research focuses on a problem called ‘Spam Bots’ by detecting the hosts that have behaviours related to spam activity. The behaviours considered in this research are as follows:

- (i) The existence of open relay service hosted on the network
- (ii) Scanning the network for SMTP service
- (iii) Disregarding mail server priority
- (iv) Connecting to multiple mail servers
- (v) Rapid connections made within a short period of time

This research focuses on these behaviours by monitoring and extracting information from the network level. The method used on the mail server connection is SMTP connection that stands on TCP protocol and the default port is (25). To correlate the detected hosts’ malicious activities, “Gower's General Similarity” is used.

1.6 Proposed Method

The research proposed method is to combine several behaviors of spam Botnet at different stages before and during spam generation. The required information to start the process of spamming is collected before the connection with the SMTP service is made, hosted by an open relay mail server on the network that is not allowed to be opened. This is achieved by:

- (i) Extracting a group of different behaviors before detecting the SMTP service and during the process of spamming on the local network. Those kinds of behaviors can be observed by monitoring the network-level traffic inside “TCP packets”.
- (ii) Proposing a set of procedures to identify the existence of compromised hosts that send out illegal e-mails (spam).

1.7 Research Methodology

The research methodology starts by determining the effective behaviours that could lead to detect Spam Bot on the network. Several studies have been done to select the most effective behaviors that are related to spam bots. The researcher has previously studied how to extract those behaviors through the proposed framework by monitoring the network traffic. Finally, studies have been done to select the best statistical formulas to measure the relations and evaluation of the proposed method.

The proposed method can be summed up into three main phases. The first phase is to capture the network traffic decoding and filtering. The second phase is to extract behaviours, and measure the relation between the detected hosts. The third

phase is evaluation, that is to check whether the related detected hosts are spam bots or not.

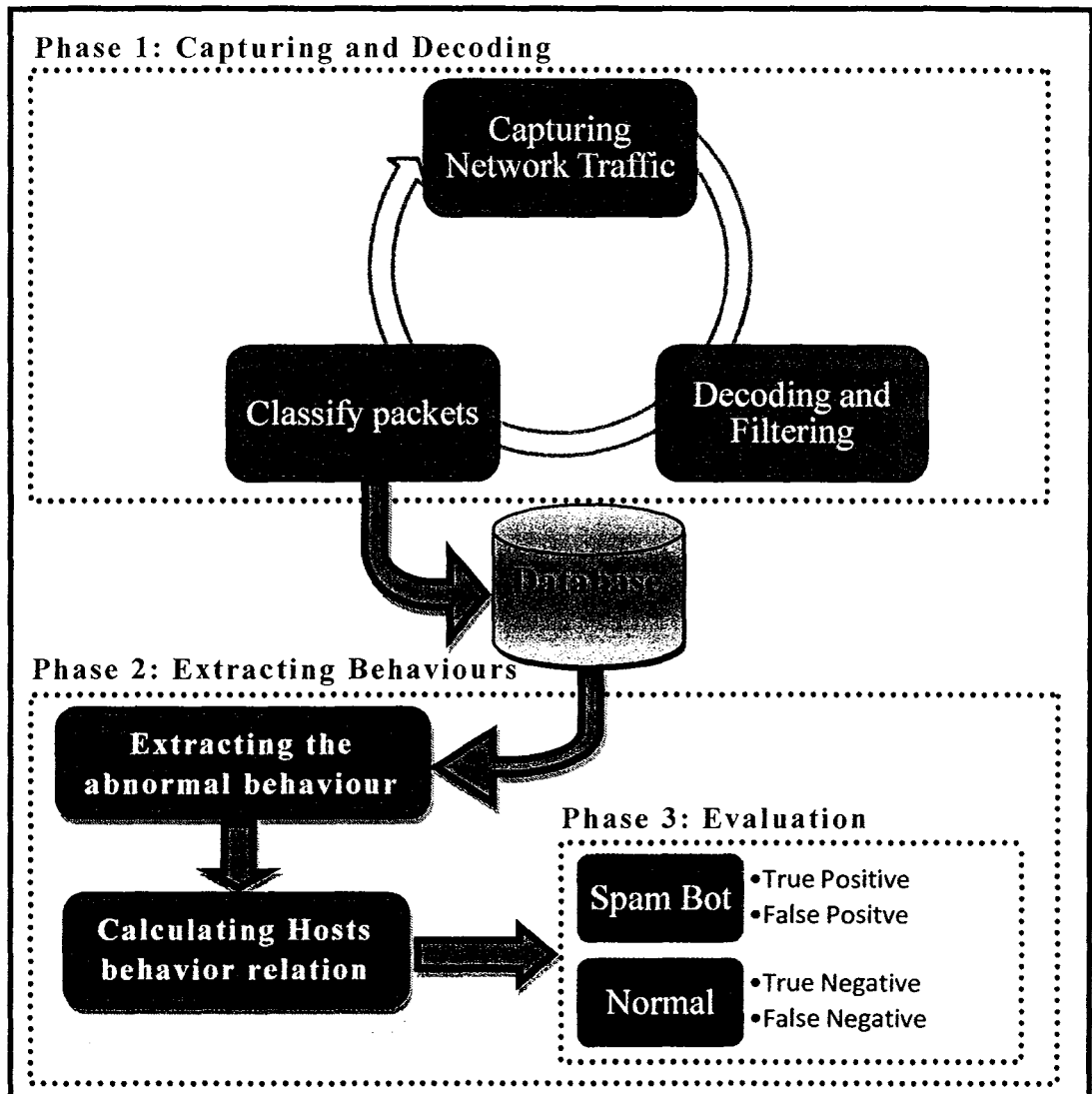


Figure 1.1: The Main Phases of Proposed Framework

1.7.1 Evaluation and Verification

To verify the proposed method efficiently, several experiments were performed in a real network environment at the National Advanced IPv6 Centre (NAv6) in USM. The proposed system monitors the network at different times to collect its different behaviours to be analysed. Several computers which had been

infected with a Spam Bot simulator reflects the same behaviour as the real spam bot. The proposed system focuses on the network traffic related to SMTP connection on the network. After that, the system collects and decodes traffic, and shows the results. There are several evaluation factors used to see how good the proposed method is in terms of performance and accuracy. The proposed system is tested whether it has met the research objectives by identifying the unwanted traffic in the network and the compromised hosts that have been involved in spamming activity. Then, it is checked whether the detected hosts that the system considers as a spam bot is a true spam bot, and also if there is any false case in terms of false positive and negative cases.

1.8 Outline of Research

This thesis consists of five chapters. Chapter One gives a brief introduction as well as a background to spam and Botnet. The contribution and objectives of the thesis are also mentioned in this chapter. Chapter Two describes the e-mail system and how it works, the main protocols used in the thesis' methodology, and the related work on spam and spam bot detection. Chapter Three explains the proposed system's procedures. Chapter Four presents the results and discusses on the findings. Chapter Five highlights the conclusion of this research, and gives the recommendations for future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter discusses in more detail how the electronic messaging system works, and the main protocols required in any e-mail sending process, SMTP and DNS. Moreover, one of the famous attacks on the network which is the network resources scanning to detect open ports in the hosts will be discussed in this chapter. The definition of open relays, several proposed solutions and previous works, that share the same goal in detecting and preventing spam, will also be discussed. Spam detection could be in different positions and techniques. As such, the main techniques are discussed in more detail in the subsequent sections.

2.2 E-mail System

Since spam is an e-mail, it has the same steps as in sending normal e-mail. This section describes how e-mail system works. E-mail system depends on multiple protocols; SMTP and DNS that are used in transmitting e-mails.

2.2.1 E-mail Sending Scenario

The e-mail sending scenario starts from the sender who sends an e-mail to the receiver by using Mail Transfer Agent (MTA) and Mail Delivery Agent (MDA) see Figure 2.1 below.

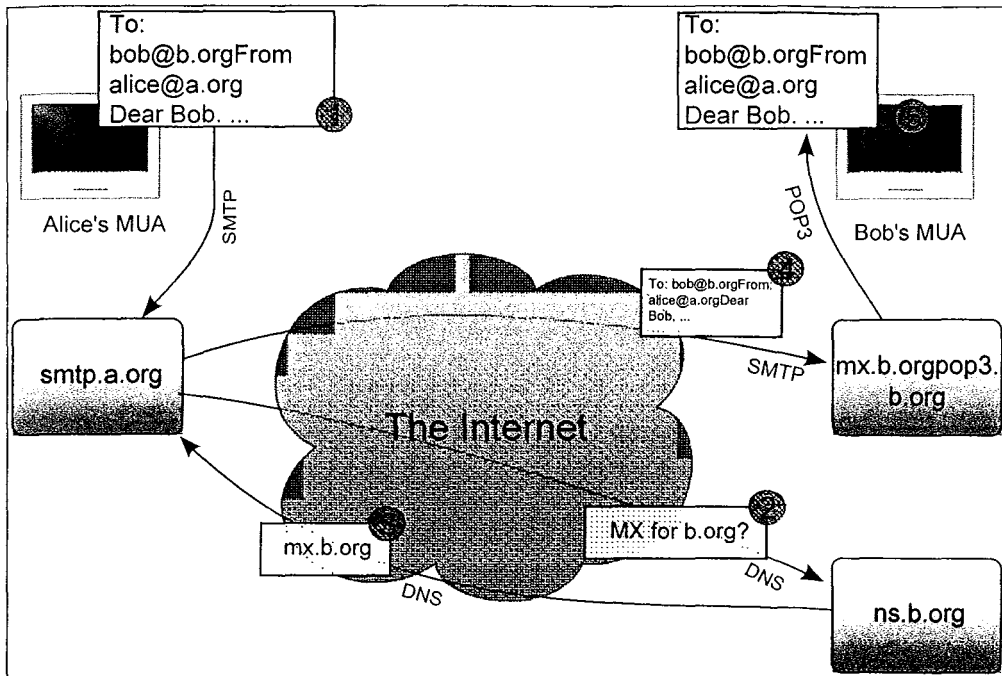


Figure 2.1: E-mails Sending Process (Wikipedia, 2007)

Initially, the mail server connects through SMTP port (25) and sends the e-mail to the Mail Transfer Agent (MTA) server which requires identifying the Mail Exchange (MX) record address of the sent e-mail. Then, the MTA sends a resolving request to the DNS server which starts searching for an MX record by sending a request to obtain the address from the distribution database. Once the address is obtained, the DNS returns the MX record to the mail server. Now, the mail server is ready to send an e-mail to the specific MX record address through the SMTP connection. Next, the receiver receives the sent e-mail through the pop3 protocol which controls the connection between the user and mail server. These concepts reoccur to each e-mail sent through the SMTP session. This information helps to understand the behaviour of spam because e-mails are sent in the same scenario which depends on two concepts; SMTP and MX queries (IBM, 2003).

2.2.2 Domain Name System (DNS) Protocol

DNS stands for Domain Name System which is the base that the Internet depends on. It converts the readable text address into an IP address. DNS query starts with the client when he/she sends a DNS query request to be resolved by the DNS server. The focus is on the requirements of the query itself (Fangming *et al.*, 2007), see Figure 2.2 below.

The main attributes in DNS query are stated below:

- (i) The Fully Qualified Domain Name (FQDN) is the root located at the hierarchy tree which ends with a dot.
- (ii) The query type determines the requested record.
- (iii) A specified class of DNS.

This research is specifically concerned with the DNS query of the Mail Exchanger 'MX' records that are used to route the e-mails.

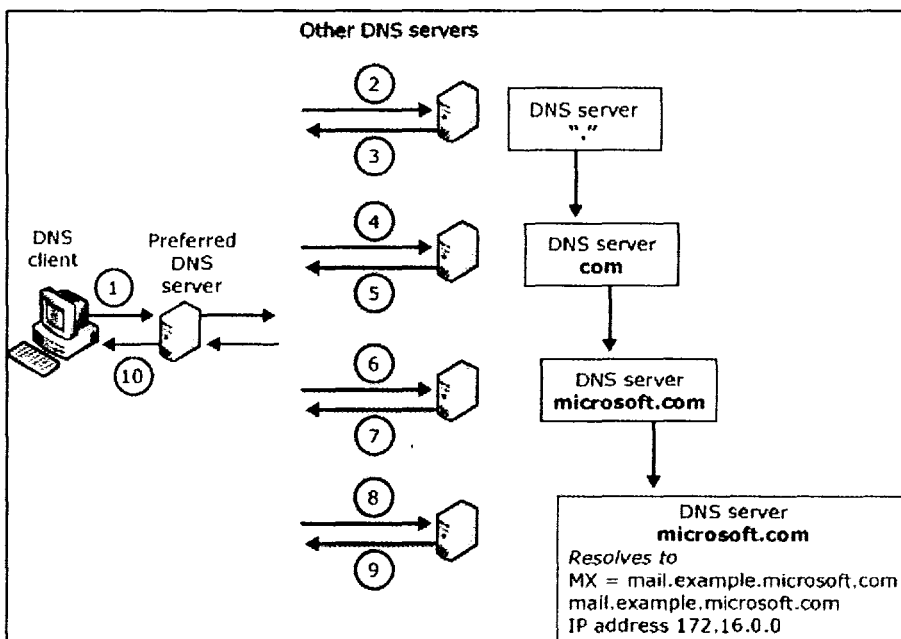


Figure 2.2: How to Resolve MX Records (Microsoft, 2005a)

An MX record includes the FQDN of the mail server zone along with a preference number from 0 through 65535. This determines the priority of the mail server. If there are multiple mail servers for the sent e-mail, the DNS query returns multiple MX records with different preference numbers. The priority of the mail servers is attached with the Dns request reply as a preference number; when the MX preference number is low, the priority of the mail server is high.

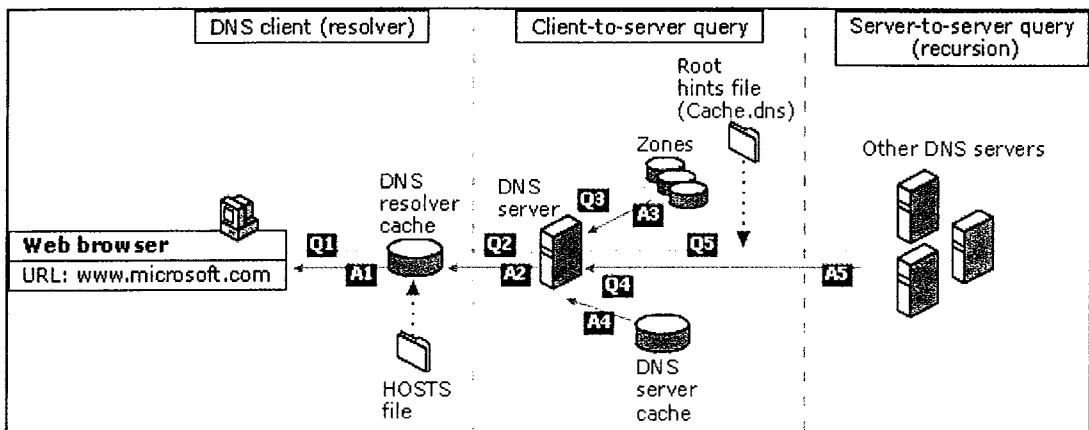


Figure 2.3: DNS Query Processes (Microsoft, 2005b)

2.2.3 Simple Mail Transfer Protocol (SMTP)

SMTP stands for Simple Mail Transfer Protocol (RFC2821, 2001) which is about how to start a connection in order to transmit e-mails with high reliability. It only needs a synchronous and reliable stream channel. TCP is the transport protocol in which the SMTP session goes through. To start an SMTP session and send an e-mail, four requirements are needed; they are listed below.

- (i) An active Internet connection to provide a connection between the client and server.
- (ii) The address of the mail server used to send the e-mail through which is usually the same domain of the sender's e-mail. For example, the domain used to send an e-mail from "fadhil@nav6.org" to any e-mail is "mail.nav6.org".
- (iii) The existence of an active e-mail receiver
- (iv) SMTP commands are implemented in order to send an e-mail.

2.3 Services Scanner Attacks

The mass mail worm depends on itself to spread and propagate in network. This is one of the security issues where a lot of research has been done to stop the worm's propagation over the networks. Worms have the ability to attack a particular TCP or UDP service port to connect and start a worm code transfer and also to compromise machines. Through the same technique, the worms keep propagating to control a large number of compromised hosts to be used later in many attacks, mostly to send spam and DDos (Avinash *et al.*, 2006).

2.3.1 Scanning Techniques

There are several techniques used in ports scanning such as TCP SYN, TCP FIN, ICMP and UDP (Arno Wagner, 2006). In this section, four of the most effective port scanning techniques are discussed below.

(a) Synchronize Packet Scanner (SYN Scan)

This technique is not a complete three handshake established connection. First, it sends a SYN packet; if the destination host is turned on and connected, it opens to respond to the packet with this flag (SYN+ACK). This reply is received by the scanner who already knows that the port is open and listens to it. The spammer uses this directly and starts sending e-mails through the SMTP commands. On the other hand, if the destination's host replies the packet with RST flag, it means that no listening is done on this port (closed port). This is a handy technique and can detect opening ports with a high percentage of accuracy.

(b) Finished Connection Packet (FIN scan)

The Transmission Control Protocol (TCP) based scanner discovers the listening port by sending FIN flagged TCP packets to the destination port wants to know if it is open, and there is a listening on it. It depends on the architectural protocol whether an open listening port receives a FIN TCP packet or no service is listening to the target port. The destination host operating system answers with an error message. If there is a service active and listening on this port, the operating system silently drops the incoming packet. This silence indicates that the service is running on the port. Because packets can be dropped accidentally in the media or can be blocked by firewalls, this detecting technique cannot guarantee open port scanning.

(c) UDP Scanning

In this case, the scanner sends an empty UDP packet. If the port is listening, the service returns an error messages or disregards the incoming packets. However, when the port is closed, most operating systems return an *ICMP Port Unreachable* message. Similar to the previous technique, this technique also does not guarantee the open port scanning and SMTP is based on TCP protocol.

(d) ICMP Scan

This technique is not a port scanning because the ICMP packet does not contain a port abstraction. Nevertheless, it is useful to determine which hosts on a network are turned on and connected by pinging the machine within a scan range using the ICMP protocol.

In this research, SYN technique is used in the proposed framework to monitor the scanning attempts in the network in this case; the scanner looks for SMTP service, in particular, on port (25) because it is the default SMTP service port.

2.4 Existing Work on Spam Detection

At present, there are many proposed and developed software and filters aimed to mitigate spamming. These are different attempts; each one has to fight spam from different places and perspectives. In lists filters for example, the white, black, and gray filters concern more with the trustable sender's address which is usually placed at the top of DNS server as in the DNSBL applications. Filters are also placed on the MDA. Usually, these filters are signatures or content-based signatures.

There are many spam detection techniques, such as lists filters, signature-based and behaviour based techniques. These techniques are further explained below.

2.4.1 White List Filter

It is a type of spam list filters that stores the list of the most trusted senders that have already gained the mail server's trust that the sender is neither a spammer nor infected with any malware that sends a huge amount of spam daily. This list gives the sender the right to classify each e-mail sent to the main inbox. This approach is widely used nowadays.

2.4.2 Black List Filter

Black list is considered as the opposite of the white list. This list filter contains the sender's IP that has already been discovered before and marked as a spammer. The spammer is kept in the black list. This technique is used by the Mail Transfer Agent (MTA); which is the first mail server that sends e-mails by using SMTP connection.

One of the well-known techniques that are being used is the DNSBL and it is used by the Mail Abuse Prevention (TrendMicro, 2008b). Basically, it is a real-time database that contains IPs of all the discovered spams such as bots and Trojans. The *DNSBL* is built at the high level of the DNS server which is the largest distributed database that contains IPs and records of names for each domain. Figure 2.4 below shows how DNS and black list work.

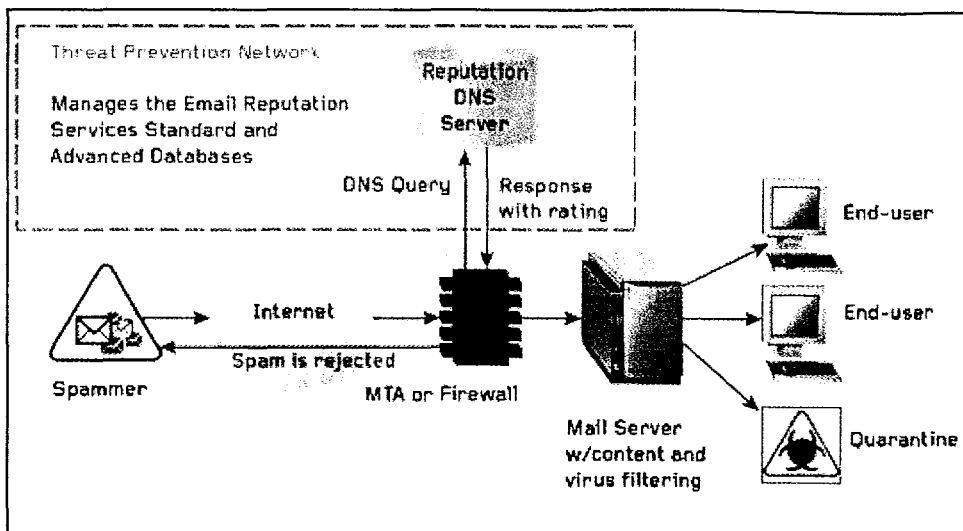


Figure 2.4: How DNSBL Works (TrendMicro, 2008a)

The record that points to the mail service is the Mail Exchanger (MX). The mail server checks for MX record that belongs to the receiver's e-mails. However, if the sender's IP is already listed in the black list, the server will reject the connection and aborts from providing the MTA with the MX record. As long as the sender does not know the MX record of the receiver; it means no e-mail can be sent. This process is achieved when the sender is considered black listed because the sender might be infected with bots or malware whose purpose is to send spams, or any other harm propagation.

2.4.3 Grey List Filter

This filter is used as a helping tool to feed lists with information. Grey listing depends on some attributes on the header of the e-mail, and observes how the e-mail behaves through the sender and receiver's addresses. Grey listing is complementary to the two previous filters (black and white filters). It simply observes the sender and recipient IP address, and postpones e-mail processing and checks if these attributes

have never been seen before. As a result, the grey list's process either rejects the SMTP connection or passes the e-mail during postponement period (Harris, 2003).

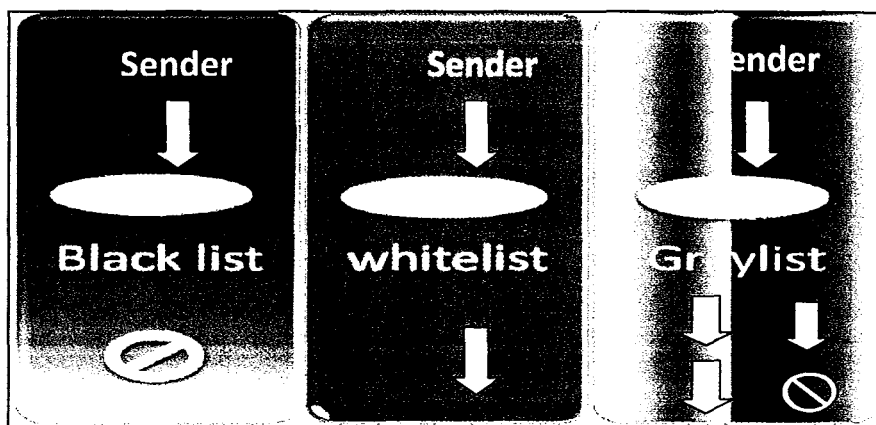


Figure 2.5: The Differences Between Black, White, and Grey Filters (Harris, 2003)

As a conclusion, the listing approach is characterized by speed and early stages of detection and prevention. However, the probability of rejecting or delaying legitimate e-mails is high. The impact of this process is, at times legitimate e-mails are classified in the bulk folder. Yet, these filters are still widely used; and there are social networks where the black and white lists can keep sharing and updating. This involves every new compromised IP which has been discovered and shared among the networks. For example, *Honeypot* is one of the well-known networks that fight spam by sharing compromised IP's.

2.4.4 Signature-based Spam Detection

This is a widely used approach in many mail server systems and it depends on some statistical methods to produce hash value, which is attached with each e-mail to become a marker or signature that classifies the e-mail. By making a comparison with the spam e-mails discovered earlier, the received e-mail is recognized and marked as a spam. Then, this e-mail hash value is stored and

distributed to all the filters that use signature technique. It is difficult to calculate the hash value because it depends on specific structures and words that e-mails contain, such as (porn materials, Click Here, Join Us) which give a suspicious value to the e-mail weight. Hash technique or signature gives accepted prevention an improbable percentage to classify legitimate e-mails as spam because it depends on the calculated hash value of the e-mails that are reported as spam.

(Kenichi *et al.*, 2004) used this hash value technique in their proposed solution. The commercial project *anti-spam* (Kaspersky, 2008) uses several detection techniques; one of the techniques is the signature-based technique. *Anti-spam* system database must be updated around the clock.

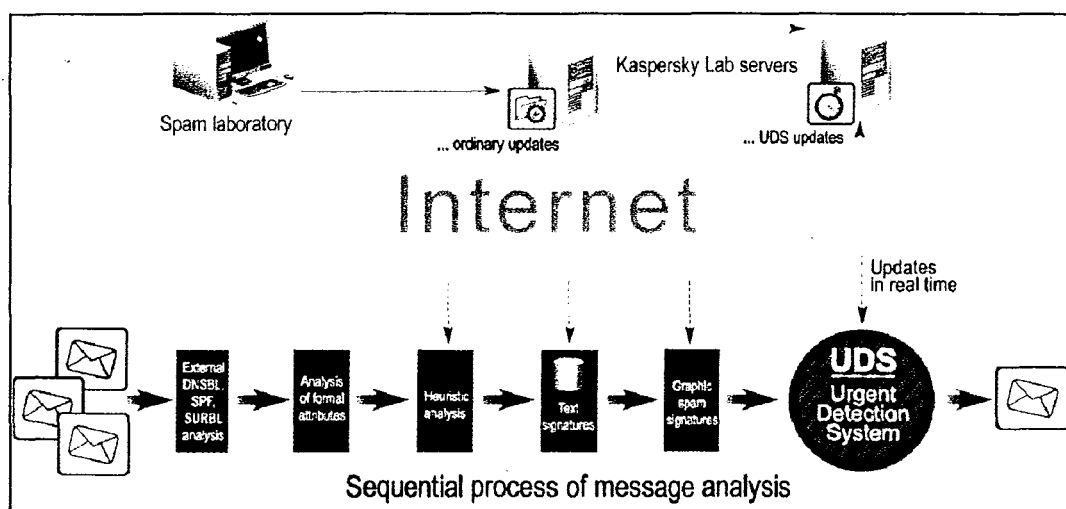


Figure 2.6: Kaspersky Anti-Spam Project Structure (kaspersky, 2008)

As shown in Figure 2.6 above, the signature needs to be updated as soon as possible to cover all the spam that are discovered recently. As discussed earlier, the social networks propagate and distribute the signature to make spam detection faster. They combine information from many spam fighters research labs.

Even though the signature technique is widely used, it only mitigates spam; unfortunately, it does not prevent them because it does not detect zero-day spam e-mails or spammers. The unwanted mail (spam) is being served and they consume bandwidth and e-mail servers' processing time. The new technique that the spammers use is to generate a text automatically and add it to each e-mail in the attempt of changing the e-mail signature or hash value to prevent being detected by the signature filters.

2.4.5 Behaviour-based Spam Detection

The rapid changes and continuous generations of new spam structure have made the effort of spam detection too difficult. Hence, this technique applies to the Botmasters that produce changeable signature spam. The signature database of the spam preventing networks i.e. *Honeypot*, cannot be updated as fast as this spam. Recently, many studies on spam prevention are focusing on how to detect spam by monitoring the behaviour of the spamming processes and observing how specific packets [DNS, TCP, and SMTP] stream on the network.

The method used by packets to characterize or extract patterns can be used as evidence of the existence of abnormal traffic or spam relays on the tested network. As mentioned earlier under the objectives and problem statement, spams can be detected before the MDA (Mail Delivery Agent) receives the mail and establishes a connection with Mail Transfer Agent (MTA).

Behaviour-based spam detection provides more ability for discovering spam in general as well as the zero-day spam. Previously, all other methods could not

detect the zero-day spams. This is because they depend on the imported pre-data in their detection system, i.e. lists-based and signature-based systems.

A group of researchers (Luiz Henrique *et al.*, 2004) studied extracting and shaping the spam on the network-level traffic by using several attributes extracted from the network level. The researchers conducted an experiment on different kinds of e-mail attributes. The information available on the header of the e-mail is used to check for any suspicious element and to identify a spam from a non-spam on the network traffic. Several behaviours can differentiate the spam e-mails in the packets stream, such as the e-mail arrival process, e-mail size, number of recipients per e-mail, and by analyzing e-mail senders and recipients. All attributes are used to provide the traffic analysis to distinguish between the traffic generated by spams and the legitimate non-spam traffic.

In their proposed solution (Jian *et al.*, 2007) stated that spamming behaviours are detected on a specific network by using two attributes. First, the probability of the compromised computer is calculated by monitoring the DNS query. After some specific observations, Jian et al's system provides the first probability value. If the probability of the monitored computer is $P(h) > 0.95$, it is considered as a compromised computer because it has a high probability from several observations of the abnormal behaviours on this computer. This is not the final decision. After this stage of analysis on the network layer, the authors went one step further by collecting information from the session layer where the data is more meaningful and useful. They used the Security Detecting System (SDS) placed at the ISP (Internet Service Provider). Table 2.1 below shows the detailed information.

Table 2.1: Log of the Security Detecting System (Jian *et al.*, 2007)

SIP	Smail	SDomain	DIP	Dmail	DDomain	Time
202.196.11 3.62	Sandra@ vip.163.c om	Vip.163.c om	61.136.58 .110	\	\	2007-2-2 11:23:13
218.68.241. 63	peter@si na.com	sina.com	209.191.8 8.247	\	\	2007-2-4 10:33:23
61.136.55.1 13	\	hexal.co m.cn	85.158.13 8.35	\	\	2007-2-2 13:41:17

This information is analysed to build a decision tree. The tree starts with checking the existence of the sender's domain and is directly divided into two branches, 1 and 0. 1 indicates the existence of the sender's real domain; and 0 indicates the fake branch value. The authors checked all the attributes to detect if there are any spam attempts.

The remaining attributes are listed as follows according to (Jian *et al.*, 2007) :

- (i) If the IP of the source domain IP matches the source domain (Type of Boolean)
- (ii) If the source domain exist (Type of Boolean)
- (iii) Receiver's named with the e-mail (Type of Boolean)
- (iv) Destination IP matches domain IP (Type of Boolean)
- (v) Number of domains used by the sender (Type of Continues)
- (vi) Number of receiver's IPs from a single sender (Type of Continues)
- (vii) The equality of IP's number with the domains used by the sender and the number of receiver's IPs (Type of Boolean).

By using Bayesian inference method, the results have proved the system's accuracy rate. The data sample and experiment information are shown in Table 2.2 below. First column shows the Training data information that used in the system

training and the second column shows the experiment's accuracy rate which is 99.56%.

Table 2.2 : Results of the Jian et al's System (Jian et al., 2007)

Training Data	Testing Data
Total Hosts: 1934	Total Hosts: 2328
Abnormal Hosts: 1705	Abnormal Hosts: 2100
Abnormal Hosts found by rules: 933	Abnormal Hosts found by rules: 1151
Abnormal hosts of 933 hosts: 894	Abnormal hosts of 1151 hosts: 1146
Rate of Recall: 52.4340%	Rate of Recall: 54.5714%
Rate of Accuracy: 95.8199%	Accuracy Rate: 99.5665%

From another perspective, in behaviour detection, which is an idea proposed by (Sandford *et al.*, 2006), they started their proposed work by finding similarity between their proposal and the way filters work. A comparison has been carried out between the bad traffic (which is referred to the network infected with some malware traffic) and the current tested network. It is assumed that there are computers on the network that are working in a legitimate manner and permitted by the ISP to use the mail servers, both local and commercial.

On the other hand, there are compromised computers infected with some type of malware which makes these computers a spam relay and probably other resources are also spying on them. (Sandford *et al.*, 2006) compared their proposed solution with the collaborate lists sharing. This is so because their solution depends on the comparison between the tested network traffics with the network traffic infected with spams.

They built a prototype that detects the illegal spamming hosts and distinguishes them from the legitimate hosts on the network by monitoring them. The system built by the authors is explained below, including how it diagnosed and obtained the results.

Firstly, this system is placed root of network; and is based on six sniffers that sniff all streaming packets on the network and also based on the central processing unit as shown in Figure2.7 below.

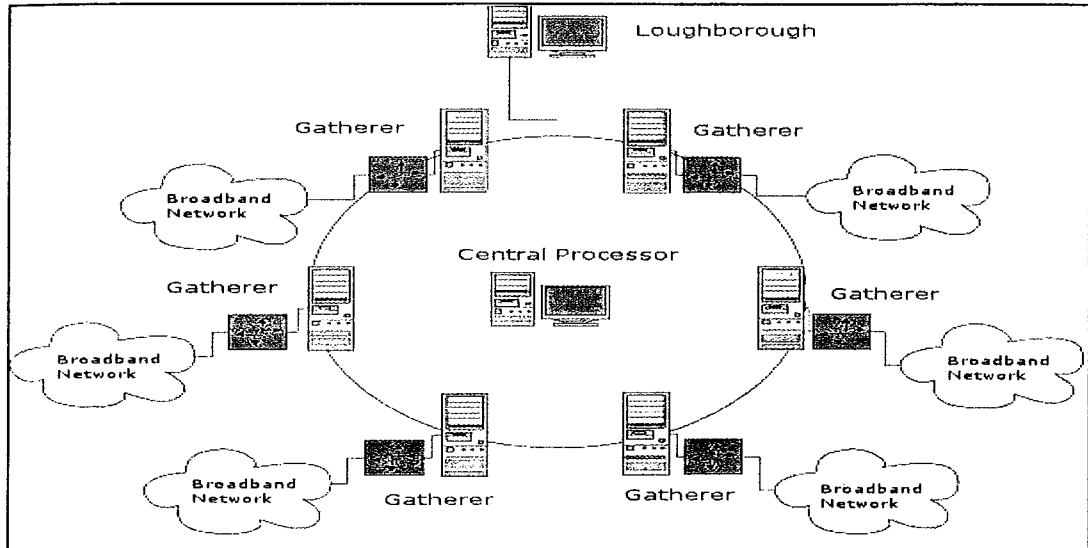


Figure 2.7 : Sandford et al's System Structure (Sandford *et al.*, 2006)

Usually the process of sending e-mails is made by https interface. Sending e-mails by using direct SMTP connection through local SMTP server or any open relay servers to distinguish between legitimate SMTP connections is not easy and needs more monitoring and observation.

A monitoring system focuses on the SMTP connections to achieve the goal which is to identify the spam relay on the monitored network. As mentioned in the introduction chapter, the application layer protocol depends on the TCP/IP transport protocol, and SMTP is a synchronous connection that uses UDP. Filtering packets depend on several rules as pointed below:

- (i) TCP/IP protocol.
- (ii) SYN (isochronized) flagged.