# INVESTIGATING PEER-TO-PEER WORM BEHAVIOR

HONG CHIN YEE

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

**BORANG PENGESAHAN STATUS TESIS**

JUDUL: **INVESTIGATING PEER-TO-PEER WORM BEHAVIOR**

SESI PENGAJIAN: **SESI 2013/2014**

Saya **HONG CHIN YEE**

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

| | |
|---|---|
| _____ SULIT | (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972) |
| _____ TERHAD | (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan) |
| ___√___ TIDAK TERHAD | |

_____ (TANDATANGAN PENULIS)

Alamat tetap :Lot 4075, Taman Pasir Panjang, 71250 Port Dickson Negeri Sembilan

Tarikh : _____

_____ (TANDATANGAN PENYELIA)

**PROF. MADYA DR MOHD FAIZAL BIN ABDOLLAH**

Nama Penyelia

Tarikh: _____

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daipada pihak berkuasa.

# INVESTIGATING PEER-TO-PEER WORM BEHAVIOR

HONG CHIN YEE

This report is submitted in partial fulfilment of the requirements for the

Bachelor of Computer Science (Computer Network)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

**DECLARATION**

I hereby declare that this project report entitled

**INVESTIGATING PEER-TO-PEER WORM BEHAVIOR**

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT :_____ Date:_____
(HONG CHIN YEE)

SUPERVISOR: _____ Date:_____
(PROF. MAHYA DR MOHD FAIZAL BIN ABDOLLAH)

# DEDICATION

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends, my supervisor and all lecturers, thanks you so much for assist and help.

# ACKNOWLEDGEMENT

Thanks to god for giving me, the opportunity to complete this Final Year Project which is titled Investigating Peer-to-Peer Worm Behavior.

First, I would like to thanks to my supervisor, Dr. Mohd Faizal Bin Abdollah for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. I also want to thanks to all lecturers for their cooperation during completing my final year project by giving valuable information, suggestion and guidance in the compilation and preparation of this report.

Next, I also obliged to staff members of Faculty of Information Technology and Communication for the valuable information provided by them in their respective fields. We are grateful for their cooperation during the period of my assignment.

Lastly, deepest thanks and appreciation to my parents, family and our friends for their constant encouragement, understanding, cooperation and full of support for completion, from the beginning till the end of the project.

# ABSTRACT

In recent year, the number of uses of the Peer-to-peer (P2P) application is with creasing and becoming popular with file sharing system, at the same time, any malicious activities in P2P network increase for example P2P worm. As the malicious software is gowthrapily, the current problem is difficult on detecting and identifying the behavior of peer-to-peer worm. Thus, the aim of this project is to investigate peer-to-peer worm behavior. This project used software and hardware tool such as Wireshark for analysis the behavior of P2P worm. The objective of this project is to investigate characteristic of worm behavior in peer-to-peer system, identify the behavior and profile of worm base on the characteristic. The project are start with literature review, analysis, implementation, finally is evaluate and testing. In the end of the project, the behavior of the P2P worn will be analysis by using control chart. Then, the control chart will evaluate based on the western electric rules.

# ABSTRAK

Kini, bilangan kegunaan bagi Peer-to-peer (P2P) adalah banyak. P2P juga menjadi popular dengan sistem perkongsian fail. Pada masa yang sama, terdapat banyak aktiviti berniat jahat atau malware di dalam rangkaian *P2P* peningkatan seperti *P2P* worm. Oleh sebab *malware* menyebar dan berevolusi dengan cepat telah menyebabkan kesukaran dalam mengesan dan mengenalpasti sifat-sifat *P2P worm*. Dalam projek ini, sifat *P2P worm* akan dikenalpasti. Projek ini menggunakan perisian dan perkakasan serta alatan *Wireshark* bagi mengumpulan data traffic untuk menjalankan analisis. Objektif projek ini adalah untuk mengaji parameter tingkah laku, mengenalpasti profil asas di dalam parameter. Projek ini dimulakan dengan kajian literatur, analisis, perlaksanaan, serta akhirnya menila dan menguji. Pada akhir projek, parameter yang terdapat di *P2P worm* akan analisis dengan menguna carta kawalan. Selepas itu, carta kawalan akan menilai berdasar peraturan *western electric.*

# TABLE OF CONTENT

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

Today, the number of uses of the Peer-to-peer (P2P) application is increasing, because it is popular with file sharing system, at the same time, many malicious activities in P2P network also increase for example P2P worm. The P2P system includes a lot of users and connectivity. Hence, P2P system probably could be potential tools to launch active worms by attackers. (Yang, Chang, Yao, & Shen, 2011).The worm exploits vulnerabilities in the host (peer) of the P2P network to affect the whole network.

## 1.2 Project Background

The worm is independent malicious software that copy itself in order to spread to other host. A worm can expand from a single copy incredibly quickly when using the internet. It's used or created by attackers to corrupt or modify the file on the host, harm the network and disruption by increasing network traffic. Therefore, peer-to-peer network become a target for the attacker.

In P2P network, the peer (host) is computer systems which are connected to each other via the Internet. A P2P worm is a worm that takes advantage of the mechanics of P2P network to replicates itself to P2P users who unsuspecting. They

spread very faster, because they do not waste the time to detect IP addresses that are not use. When a user request or search a file, P2P network try informing remote users of the file. The user will start download after remote user share the file to the user.

Mostly, P2P worm will generate low rates of failed connections only. Hence, the normal traffic patterns of the P2P network will integrated by them. The abnormal network will hard to detect cause P2P worms could be potentially threat because ineffective to existing defence mechanisms for worm detecting or scanning the worm (Zhou et al., 2005).

Furthermore, worm like to attack the environment where has many connectivity. Therefore, P2P application becomes the target for worm. It gets severe after it takes action to overcome it. Nevertheless, the research will be observe how the worm goes before the precaution is carry out.

Thus, the research focuses on the analysis of the worm in peer-to-peer (P2P) network and how the P2P worm interactive in P2P network. The changes in the network can be detected by analysis abnormal traffic behavior. In this project, the parameter such as header of the packet and network traffic will be investigated.

## 1.3 Problem Statement

Worm attack in peer-to-peer network will spread widely, rapidly; the network will affected by embed to the whole connectivity in P2P network. The parameter of the network traffic becomes a key issue of the research. It may cause the behaviour of the worm will difficulty to detect and identify. The Research Problem (RP) is summarized in Table 1.1.

**Table 1.1 : Summary of the Research Problem**

| No. | Research Problem |
|---|---|
| **RP1** | Difficulty in detecting the behaviour of Peer-to-Peer worm |

## 1.4 Research Question

Based on Table 1.2, there are two Research Questions (RQ) is form to determine the problem statement as discussed in the previous section.

**Table 1.2 : Summary of Research Question**

| RP | RQ | Research Question |
|---|---|---|
| RP1 | RQ1 | What is the behavior of peer-to-peer worm? |
| | RQ2 | What is the network parameter use to identify profile and the behavior of peer-to-peer worm? |

**PQ1: What is the behavior of peer-to-peer worm?**

This research question is to study and find out the suitable method that needs to use to collect the data which use to determine the behavior of the worm.

**PQ2: What is the network parameter use to identify profile and the behavior of peer-to-peer worm?**

This research question is to study the behavior of the P2P worm by analyze suitable parameter. The parameter should be use in the research is important because different parameter may infect by type of worm.

## 1.5 Research Objective

Two research question that constructed in the previous section, appropriate research objectives (RO) are summarized in Table 1.3.

**Table 1.3 : Summary of Research Objectives**

| RP | RQ | RO | Research Objective |
|---|---|---|---|
| PP1 | RQ1 | RO1 | To investigate characteristic of worm behavior in peer-to-peer system |
| | RQ2 | RO2 | To identify the behavior of worm base on the characteristic. |
| | | RO3 | To identify the profile of worm base on the characteristic. |

## 1.6 Project Scope

The project will be focus on:

a. peer-to-peer worm
b. Characteristic of peer-to-peer worm
c. Define the control chart

## 1.7 Project Significant

This project will be a significant endeavour in analyzing abnormal data packets in network traffic. This project will also greatly benefit the professionals and those who are going to involve in this area of work in terms of analyzing the type of abnormalities of data in network traffic. This project can be a guideline for them in the future research.

## 1.8 Expected Output

There are several research scopes of this study:

i. This project will be held on UTeM's environment that accounting the P2P hardware and software ability. The project will be conduct by using the environment that testing and evaluating the P2P computing network based on the several of characteristics.

ii. This study focuses on normal traffic and abnormal traffic that was captured in the real P2P network traffic.

iii. The real P2P network traffic is runs on Microsoft Windows 32-bit platforms.

iv. This study also only focuses on P2P worm characteristics analysis by comparing the new characteristics between P2P normal and P2P worm.

v. To differentiate the new characteristics, this study uses the several of open source network analysis tools as it's provide the necessary features. These features are useful to distinguish if any network violations are occurring.

vi. In addition, the project can increase the awareness and knowledge on P2P worm and encourage community participation.

## 1.9 Report Organization

**Chapter 1: Introduction**

This chapter will discuss about overview introduction, background of the research, problem statement, research question, research objective, project scope, project significant and expected output.

**Chapter 2: Literature Review**

This chapter will explain related the work of this research, such as peer-to-peer, worm, analysis technique, parameter pervious work and current work.

**Chapter 3: Methodology**

This chapter will discuss the method use to analyze the peer-to-peer worm and organize the sequence of project work in phase by phase.

**Chapter 4: Implementation**

This chapter will introduce the software and hardware used in this project, environment setup, implementation of worm as well as the data collected.

**Chapter 5: Testing**

This chapter will analyze the other collected data and compare with pervious traffic to support the evidence.

**Chapter 6: Conclusion**

This chapter will provide conclusion and summary of the project, limitations, contribution and the future work of the project.

## 1.10 Conclusion

In conclusion, this research will define the parameter to study the behavior of the P2P worm based on the network traffic. The research problem, research questions and objective of the projects are clearly discussed in this chapter. The related work of the research wills discuss more depth in next chapter which is literature review.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

In previous chapter, the research problem, research questions and research objective of the research are clearly discussed. In literature review, the related work of the research will be discussed. The objective of this chapter is to find out several issues that related to this research, such as peer-to-peer, worm, analysis technique and also include pervious and current research as depicted in Figure 2.1.

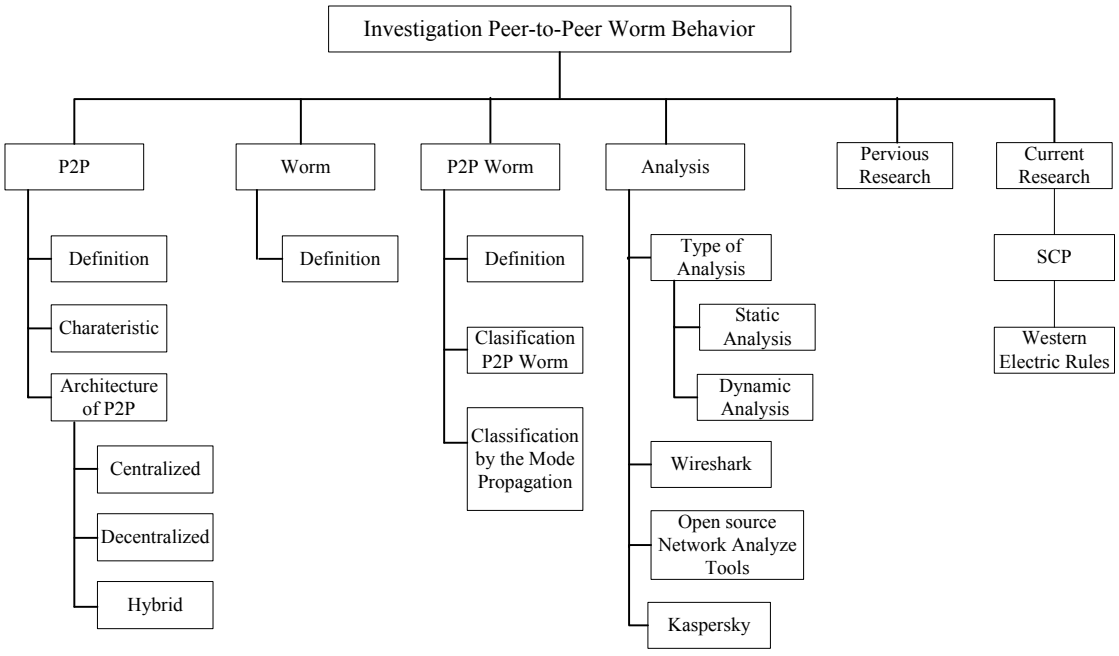


**Figure 2.1 : Operational framework: Literature review phase**

## 2.2 Peer-to-Peer

The detail description of the P2P is discussed in this section. The definition of the P2P will be defined. Moreover, this section also will find out characteristic and taxonomy of P2P.

### 2.2.1 Definition

Each of the peers in peer-to-peer has the same capabilities in communication network. It can start a communication session and able to direct exchange resources and services between themselves (Margaret Rouse, 2009). Client and server model is type of the P2P model. Each of the client and server can communicate to each other with giving each capability.

In network, the computer, node can be divide into two which is server and client. The absence of centralized authorities in P2P networks results in a totally distributed configuration of directly connected peers.

### 2.2.2 Characteristic

(Loo, 2007) illustrated some common characteristics shared by most P2P technology:

a. A computer can call it as peer that can act as server and/or client. In particular time, the requirement of the system will determined the peer.
b. P2P is freely system, because peers can leave or join easily. After join the network, peers should be able to exchange resources directly between themselves such files, storages, information, central processing unit (CPU) power and knowledge.
c. In P2P network, then number of the peer should not be less than 2 and the maximum number of peer are infinity.
d. Peers may belong to different owners. It is common for P2P systems to have several millions of owners.

e. Dedicated servers may or may not be present in a P2P technology depending on the nature of the applications.

### 2.2.3 Architecture of P2P

As the architecture of a system is the cornerstone of high-level applications that are implemented upon it, an understanding of P2P architecture is essential to gaining its full potential. Its enables we to determine the architectural factors that are critical to a P2P system's performance, reliability, scalability, and other features. Therefore, we dedicate this chapter to summarize and examine the architecture of P2P.

#### 2.2.3.1 Taxonomy

Taxonomy is derived from examining existing P2P systems. In general, we can categorize the systems into two broad categories, centralized vs. decentralized, based on the availability of one or more servers, and to what extent the peers depend on the services provided by those servers. Besides these two main categories, there are also hybrid P2P systems which combine both centralized and decentralized architectures to leverage the advantages of both architectures (Quang Hieu Vu, Mihai Lupu, 2010). Figure 2.2 shows the taxonomy.

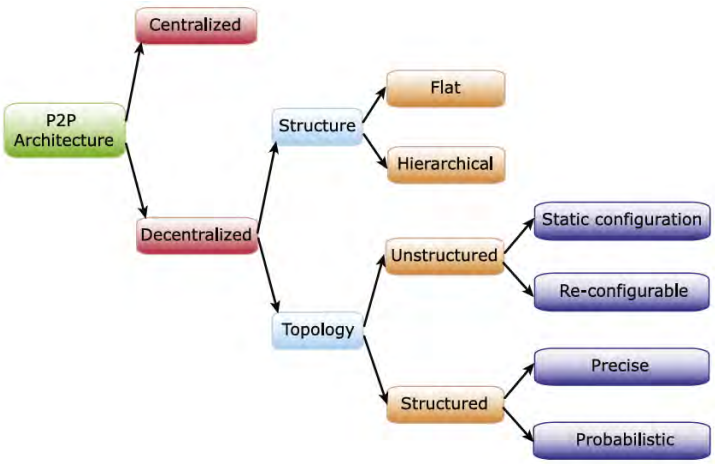


**Figure 2.2 : A taxonomy of P2P systems (Quang Hieu Vu, Mihai Lupu, 2010)**

**a. Centralized P2P**

Like a client-server system, there are one or more central servers, which peer to locate their desired resources or act as task scheduler to coordinate actions among them. To locate resources, a peer ends messages to the central server to determine the addresses of peers that contain the desired resources or to fetch work units from the central server directly. The logical design is show on Figure 2.3.

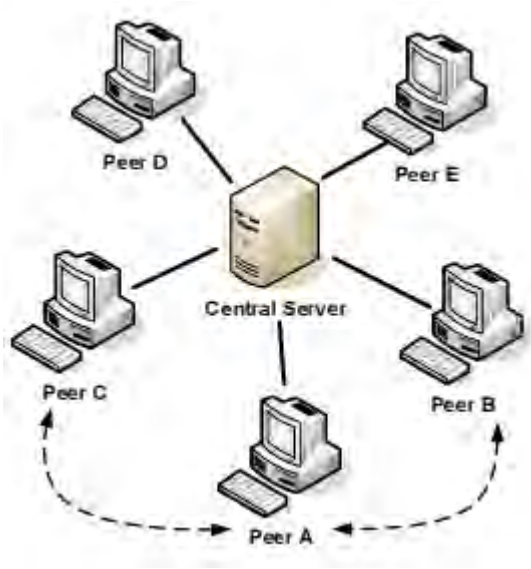


**Figure 2.3 : The centralized P2P Network (Quang Hieu Vu, Mihai Lupu, 2010)**

As in all centralized systems, these categories of P2P systems are susceptible to malicious attacks and single point of failure. Moreover, the centralized server will become a bottleneck for a large number of peers, potentially degrading performance dramatically. Finally, this type of system lacks scalability and robustness (Quang Hieu Vu, Mihai Lupu, 2010)

**b. Decentralized P2P**

In a decentralized P2P system, peers have equal rights and responsibilities. Each peer has only a partial view of the P2P network and offers data/services that may be relevant to only some queries/peers. The advantages of these systems are immune to single point of failure, and possibly enjoy high performance, robustness, scalability.