Simulation Modelling Practice and Theory 51 (2015) 87–99

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Modeling and analysis of passive worm propagation in the P2P file-sharing network

Chao-sheng Feng [a,b,*], Jun Yang [a], Zhi-guang Qin [b], Ding Yuan [a], Hong-rong Cheng [b]

[a] School of Computer Science, Sichuan Normal University, Chengdu, Sichuan 610101, China
[b] School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 610054, China

ARTICLE INFO

Article history:
Received 31 August 2014
Received in revised form 4 November 2014
Accepted 7 November 2014
Available online 8 December 2014

Keywords:
Passive worms
Modeling propagation
P2P networks
Reproduction number
Worm free equilibrium

ABSTRACT

A number of worms, named P2P (peer-to-peer) passive worms, have recently surfaced, which propagate in P2P file-sharing networks and have posed heavy threats to these networks. In contrast to the majority of Internet worms, it is by exploiting users' legitimate activities instead of vulnerabilities of networks in which P2P passive worms propagate. This feature evidently slows down their propagation, which results in them not attracting an adequate amount of attention in literature. Meanwhile, this feature visibly increases the difficulty of detecting them, which makes it very possible for them to become epidemic. In this paper, we propose an analytical model for P2P passive worm propagation by adopting epidemiological approaches so as to identify their behaviors and predict the tendency of their propagation accurately. Compared with a few existing models, dynamic characteristics of P2P networks are taken into account. Based on this proposed model, the sufficient condition for the global stability of the worm free equilibrium is derived by applying epidemiological theories. Large scale simulation experiments have validated both the proposed model and the condition.

1. Introduction

P2P networks have become popular recently because they can not only facilitate disseminating sources or sharing files with considerable scalability and reliability, but also effectively solve the problem of service bottleneck, which can not be solved in client/server networks. The measurements show that the traffic from P2P networks has accounted for more than 60% of the overall Internet traffic [1,2]. Among all the existing P2P networks, P2P file-sharing networks enjoy the most popularity. Such P2P file-sharing networks as eMule [3] have over ten million users and the number of online users at any given time is more than two million.

However, the appearance of dozens of P2P passive worms which propagate on P2P networks has posed heavy threats to such networks [4]. In contrast to the majority of traditional Internet active worms like the Slammer and Blaster which actively connect to victims, it is by exploiting user's legitimate activities such as downloading instead of vulnerabilities of networks on which these worms passively propagate. This passiveness evidently slows down their propagation, which results in them not attracting adequate attention in literature. Meanwhile, this passiveness visibly increases the difficulty of detecting them, which makes it very possible for them to become epidemic.

* Corresponding author at: School of Computer Science, Sichuan Normal University, Chengdu, Sichuan 610101, China.
E-mail addresses: csfenggy@sicnu.edu.cn (C.-s. Feng), yanghuajun@163.com (J. Yang), qinzg@uestc.edu.cn (Z.-g. Qin), yuanding123456@gmai.com (D. Yuan), hrcheng@uestc.edu.cn (H.-r. Cheng).

http://dx.doi.org/10.1016/j.simpat.2014.11.004
1569-190X/© 2014 Elsevier B.V. All rights reserved.

P2P passive worms and their threats have been studied in literature and several models for P2P passive worm propagation have been proposed as well. While studying on some worm and prevention of the worm, proposing models suitable for the worm propagation is usually the first task, because good models, which are proposed based on the analysis of attacking and spreading mechanisms of the worms and properties of the network in which the worm spreads, can fully expose behaviors of the worm, identify vulnerabilities of the worm propagation chain, and predict the tendency of its propagation. Although these existing models are really reasonable to some extent, they all have the same weakness that the dynamic characteristics of P2P networks, such as users joining networks and users leaving networks, are taken into account little or even ignored. This weakness not only reduces the validity of these models, but also necessitates proposing a new model of P2P passive worm propagation in which the dynamics of P2P networks are considered. Given this, we thoroughly studied on P2P file-sharing networks, especially their dynamics and passive worms in them, and contribute the following.

(1) Model propagation of P2P passive worms with consideration of the dynamics of the P2P network.
(2) Derive the sufficient condition for the global stability of the worm-free equilibrium.
(3) Validate the proposed model and verify the sufficient condition with large scale simulation experiments.

The rest of this paper is organized as follows. We discuss the existing studies of worm propagation in Section 2. In Section 3, we model propagation of P2P passive worms. The sufficient condition for worm-free equilibrium is derived in Section 4. In Section 5, we evaluate the performance of the proposed model and the derived sufficient condition by comparing theory results with simulation results. In addition, we examine the effect of P2P-related parameters on the evolution of the prevalence of passive worms. Finally we conclude and discuss the future work in Section 6.

2. Background

2.1. Related study

In 2002, Staniford et al. presented the concept of P2P worms [5]. They concluded that P2P systems are well suited for worm propagation. However, they did not give any detailed analysis or model the propagation of P2P worms. In 2003, Guammadi found that the popularity of P2P files follows a Zipf distribution [6]. Sarious found that P2P networks are highly dynamic [7]. In 2004, Yu gave an analytical model for P2P worms in the discrete-time method and examined the effect of different parameters on the worm propagation [8]. Zhou studied worm propagation with a simulation framework that implemented several protocols as Gnutella, Gia and Pastry [9]. But both Yu and Zhou focus on P2P active worms. There have been a number of papers which model file propagation in P2P networks. Two notable examples include a 2004 paper by Qiu and Srikant [10] which models the performance of the BitTorrent P2P protocol and a 2005 paper [11] by Dumitriu et al. which models the spread of polluted files in P2P networks. In 2005, Thommes et al. modeled virus propagation and pollution file spread in P2P networks by applying Epidemiology, respectively [12]. Although they claimed that they had derived a dynamic model to describe the evolution of infection, in fact, the dynamic properties of the P2P network are considered little; thus, the proposed models are inadequate in terms of validity. In 2006, Stutzbach et al. presented a detailed study using three widely-deployed P2P systems: an unstructured file-sharing system(Gnutella), a content-distribution system (BitTorrent), and a Distributed Hash Table (Kad). Their study revealed that P2P networks are highly dynamic [13]. Chen pointed out that P2P worms are non-scanning worms and identified three types of P2P worms: passive worms, reactive worms and proactive worms. In order to characterize P2P worms and examine the impact of P2P-related parameters on worm propagation, they also developed a workload-driven simulation framework. Yet mathematical models of P2P worm propagation were not presented in their paper [14]. In 2008, Wang et al. proposed a mathematical model for the propagation of passive worms over Gnutella [15]. An evident drawback of their work is the assumption that the whole network has a static topology, in other words, there is no consideration on dynamic changes of the network. A virtual-node based simulation approach and a double-engine based simulation architecture [16] were proposed for simulating large-scale P2P worms by Wu and Qin. In 2012, Feng et al. presented an analytical model suit for P2P reactive worms [17]. Yan et al. proposed a modeling and analysis method of containing worm propagation in P2P network based on stochastic process algebra [18]. In 2013, Mojahedi et al. presented a propagation model of topology-aware P2P worms (also called P2P active worms and P2P proactive worms) [19]. In this proposed model, these factors of topology, configuration, countermeasures and defense strategies as well as infection time lag, were considered. At the same time, Chen et al. proposed a propagation model for P2P active worms, based on the ternary logical matrix [20]. In 2014, Jafarabadi et al. introduced a stochastic and discrete-time model for topology-aware active worm propagation with consideration of the join and leave of hosts [21]. However, these study paid attention to P2P active worms rather than P2P passive worms. In the same year, Chen et al. took address hiding, configuration diversity, online/offline behaviors and download duration into account during modeling and proposed a Four-Factor propagation model of p2p passive worms [22]. But they did not simulate practical P2P networks and propagation of P2P passive worms.