Applied Mathematics and Computation 229 (2014) 340–349

Contents lists available at ScienceDirect

Applied Mathematics and Computation

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

Capturing the interplay between malware and anti-malware in a computer network

A.K. Misra *, Maitri Verma, Anupama Sharma

Department of Mathematics, Faculty of Science, Banaras Hindu University, Varanasi 221 005, India

ARTICLE INFO

Keywords:
Mathematical model
Computer networks
Malware
Anti-malware
Stability

ABSTRACT

In an era with affluence of local area networks, the recurrent attacks of viruses and other malicious objects are undoubtedly an intruding threat. These malicious objects spread quickly through an unprotected network, corrupt the data and harm the nodes. To comprehend this problem and its plausible solutions more thoroughly, we have proposed and analyzed a mathematical model by considering a network in which nodes are either infected or prone to it. It is considered that nodes vulnerable to infection become infected, when attacked by malicious objects present in the network. To minimize the abundance of malicious objects and infected nodes, some anti-malware softwares are installed in the network, which are continuously being updated. On analyzing the proposed model, we obtained two equilibria and a threshold governing the dynamics of malicious objects in a computer network. The characterization of stability behavior of obtained equilibria is also discussed in detail. The numerical simulation illustrates the validity of analytically obtained results.

1. Introduction

With the evolution of computer networks, the need of protecting files and other information stored on the computers have become imperative. Peer-to-peer file sharing amongst operating systems and other widely distributed network softwares provide favorable conditions for malicious attacks. Due to this, the spread of viruses, worms, Trojans and other malicious softwares have increased dramatically in the last decade. Malicious softwares or malwares are the programs written with an intention to cause some kind of damage to computer systems and networks. Computer viruses are most widely recognized class of malware. Once a virus enters any computer or network, it performs two functions: it infects other programs by copying itself and it executes malicious codes those have been included by author in it. These viruses are especially designed to damage the system and their effect can be so extensive that the complete rebuilding of all softwares and data may be required. Due to the swift spreading nature of computer viruses, the damage can multiply in the network topology within a fraction of time.

The computer viruses have acquired this name due to their resemblance with the biological viruses. Biological viruses transmit from person-to-person, while computer viruses pass from computer-to-computer. A biological virus is a fragment of DNA inside a protective jacket, which injects its DNA into a cell to reproduce itself. A computer virus does the same. It attaches itself to some program or file in order to get executed that works as a host for it. When the user runs the infected program or file, the virus becomes alive and, start replicating and infect other programs or files on the computer, [1]. A virus transmits from the infected computer to an uninfected one, when its host is transmitted to the uninfected computer either

* Corresponding author.
E-mail address: akmisra@bhu.ac.in (A.K. Misra).

0096-3003/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.amc.2013.12.059

by sending it over a network or by transferring it through removable media such as a floppy disk, CD[1] or USB[2] drive. Meanwhile viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Other widely prevailing variants of malware are computer worms and Trojan horses. A worm can spread itself to other computers without needing to be transferred as part of a host whereas a Trojan horse is a file that appears harmless but it enhances the system vulnerability.

To hinder any potential threat of malicious attack, the anti-malware softwares are installed on the system those can detect and eliminate malwares from the system. An anti-malware software detect viruses and other malicious objects using a list of malware signature definitions. It examines the content of the computer's memory and files stored on the drives, and compare them with a database of malware signatures. Due to this, a system is only protected from malwares those were known before the last malware definition update. Therefore, the potency of anti-malware software depends heavily on whether these malware definitions are updated in a timely manner or not. Thus, there is a need to continuously update and maintain a latest database of malware signature, to maximize the functionality of anti-malware against new threats.

Understanding about the spread of computer malwares (virus, worms, Trojans, etc.) in a network has increased significantly in the last decade. The dynamics of computer viruses spread is analogous to the viruses of biological diseases and therefore the same notion can be applied to the spread of computer viruses, [2]. Various mathematical models have been devised using the epidemiological approach to study the effect of viruses and other malicious objects on the computer networks [3–10, and references therein]. The incorporation of time delays in epidemiological model for computer virus gives rise to rich and interesting dynamics [11,12]. A motive behind modeling of an epidemic is gaining comprehensive knowledge about its transmission so that effective intervention strategies can be devised for its control. Similarly, for computer virus also, various defence mechanisms like; anti-virus [13,14], antidotal computers [15], intrusion detection system [16], are employed to mitigate network vulnerabilities and ensure its security. Recently, Mishra and Keshri [17] have investigated an e-SEIRS model with vaccination to study the effect of worm attacks on sensor nodes in a wireless sensor network. They found that regular use of antivirus software in the sensor nodes of the sensor field make the defense mechanism strong and hence minimize the potential threat of worms.

All these studies have used the concepts of population dynamics to model the transmission dynamics of virus in a computer network. However, as mentioned above, the dynamics of a computer virus is akin to that of a biological viruses. So, it is more realistic to model the spread of viruses and other malware in a computer network using an approach similar to viral dynamics *in vivo* [18–21]. The main focus of this study is to assess the potency of anti-malware softwares in protecting a computer network from malicious attack. We have organized the rest of the paper as follows: Section 2 presents the mathematical model with rationale of all the assumptions. Section 3 and 4 contain the equilibrium and stability analysis, respectively; and Section 5 presents the numerical simulation. Section 6 summarizes the principal findings of the present work.

2. The model

Consider a computer network comprising some nodes, all uninfected but vulnerable to any malicious attack. When a malicious software hits this network, some nodes become infected. These infected nodes work as a reservoir for the malicious objects, in which they replicate and hence the abundance of malicious objects increases. The presence of these malicious objects in a network has devastating consequences on software such as, data corruption, programs malfunctioning as well as hardware like, crashing of nodes. Therefore, anti-malware softwares are installed on the system, so that they can keep any malicious threat at bay. Due to the emergence of new malware, the anti-malware needs to be regularly updated in order to recognize the latest threats and maintain their potency.

Let us assume that there are $N(t)$ nodes present in the network at any time t. Depending upon the state of infection, all the nodes are divided into two subclasses namely; susceptible S and infected I. Further, consider that $M(t)$ denotes the number of malicious objects in the network at time t and $P(t)$ measures the potency of anti-malware softwares at time t. Consider that naive nodes are being installed in the network with a constant rate A and nodes are being removed from the network due to crashing or other system failure with a rate dN, where constant d represents crashing rate. Moreover, the infected nodes are more vulnerable to crashing and system failure, so their removal rate is assumed to be greater than that of susceptible nodes and the constant α denotes this malwares-induced crashing rate. The malicious objects are attacking the susceptible nodes due to which susceptible nodes are becoming infected with a rate βSM. It is further assumed that the infected nodes are being cleaned by anti-malware software due to which they recover and leave the infected class with a rate γIP. The wealth of malware in the network depends primely upon two factors *viz.* how many computers are infected in the network and how fast a virus can copy itself. Therefore, the evolution of malicious objects in the network is assumed to be dependent on the number of infected nodes I and replication potential of malware k, and hence the growth rate of malicious objects in the network is assumed to be $k\phi I$, where ϕ is invasion rate of malwares. The anti-malwares act upon these malicious objects and lessen their abundance with a rate $\phi_0 MP$. Therefore, the diminution rate of malwares depends upon the removal rate of malicious objects by anti-malwares, ϕ_0, number of malwares, M itself and most importantly on the potency of anti-malware, P. Thus, the presence of a high number of infected nodes signifies presence of high number of malwares in the network, which

[1] Compact disk.

[2] Universal serial bus.