International Journal of Information Security and Privacy
Volume 13 • Issue 1 • January-March 2019

Behavioral Modeling of Malicious Objects in a Highly Infected Network Under Quarantine Defence

Yerra Shankar Rao, Gandhi Institute of Excellent Technocrafts, Deuliapatna, India
Prasant Kumar Nayak, C. V. Raman College of Engineering, Mahura, India
Hemraj Saini, Jayppe University of Information Technology, Waknaghat, India
Tarini Charan Panda, Ravenshaw University, Cuttack, India

ABSTRACT

This article describes a highly infected e-epidemic model in a computer network. This article establishes the Basic reproduction number R0, which explicitly brings out the stability conditions. Further, the article shows that if R0< 1 then the infected nodes ceases the spreading of malicious code in computer network as it dies down and consequently establishes the asymptotically stable, when R0> 1, the alternative aspect is that infected nodes stretch out into the network and becomes asymptotically unstable. The pivotal, impact of quarantine node on e-epidemic models has been verified along with its control strategy for a high infected computer network. In the MATLAB simulation, the quarantine class shows its explicit relationship with respect to high as well as low infected class, exposed class, and finally, with recovery class in order to yield increasing safety measures on transmission of malicious codes.

KEYWORDS

Basic Reproduction Number, Computer Network, E-Epidemic Model, Quarantine, Stability Condition

INTRODUCTION

Presently a day, number of internet users has increased rapidly and around 41% of the world population are using internet today. Every internet user knows what malicious code is (popularly called virus) and its impact to computer security. But many of them don't know how these viruses enter to computer and how they spread in the computer network moreover how long these viruses work in computer system. Answer of first one is that, there are many ways in which a virus can enter in a computer network, such as e-mail attachments, fraud Websites, contaminated boot software, phishing Schemes, pirating activist, social network, etc. In these days many people are busy with social network site for their communication, some popular social network sites are Facebook, twitter, LinkedIn, Google+, and many more. These social network sites are the latest targets of hackers to deliver computer

DOI: 10.4018/IJISP.2019010102

viruses. Once a virus enters to one computer then it is easily spread throughout the network. Worm/virus attack is considered by network experts the highest risk in terms of functionality and assets. Attacker use malicious worm as primary tool to make the software vulnerable. In order to have a better grip from the security concern, one should regularly update the anti-virus software even if their computer noticeably infected and timely disconnected the computer from the internet, whenever this connection is unnecessary. Also filtering and blocking suspicious message with firewall is reward.

The use of a quarantine strategy has confirmed great attention to get rid of disease spread, and thus adapted to protect a system against worms. In the faculty of computer, the use of quarantine measures depends on an intrusion detection system (IDS). The IDS has two parts, first, a misuse IDS and second, an anomaly IDS. The anomaly detection system is generally used to notice malicious code such as computer viruses and worms, to ensure relatively appreciable performance. In such a system, the normal system behavior database is built prior. Once a divergence from the normal behavior is observed, such behavior is considered as an attack, and a suitable comeback action, such as vaccination and quarantine are prompted.

Quarantine process is a substitute method to reduce average infectious period by isolating some infection so that they do not transmit the malicious object in the computer network. Concern to the approach, R_0 decreases with increase in quarantine rate.

Since the spreading nature of malicious codes are just like biological virus therefore, the involvement of malicious codes inside the network can be studied (Divya & Padmavathi, 2014; Gan et al., 2013; Han & Qiulin, 2010; Hethcote et al., 2002; Kumar et al., 2015; Madar et al., 2004; May & Lloyd, 2001; Michael et al., 1999; Newman et al., 2002; Piqueira et al., 2005; Ren et al., 2012; Rao et al., 2016; Rao et al., 2017; Xiaofan & Lu-Xing, 2012; Yang et al., 2013; Yuan & Guoqing, 2008) by using epidemiological models for disease spread (Datta & Hui, 2005; Keeling & Ken, 2005; Kermack & McKendrick, 1927; Kermack & McKendrick, 1932; Lahrouz et al., 2012; Mishra & Jha, 2010; Ping & Shengqiang, 2006). Recently, intense research activity has been observed for the combination of virus propagation model and antivirus countermeasures to estimate the prevalence of virus, e.g., virus immunization (Saini & Saini, 2007; Thommes & Mark, 2005; Toutonji et al., 2012; Wu & Zhilan, 2000; Yang & Xiaofan, 2014; Zhu et al., 2012; Zhu et al., 2013) and quarantine (Gan et al., 2012; Mishra & Pandey, 2012; Mishra & Prajapati, 2014). This article focus mainly represents an impact of virus on computer security and how long they work in the computer network and under what strategy we can protect our computer from the virus attack.

This further text is organized in different other sections as; section-2: a mathematical modeling has been explained explicitly, section-3: it derives the basic reproduction number along with its significance, section-4: existence of equilibria and analysis of dynamic behavior has been covered and in section-5: mathematical results are put forwarded abided with numerical simulation along with some control strategy, and finally it summaries the approach and proposes the future scopes.

NOMENCLATURE

N (t): Total number of computer nodes interacting continuously with each other at time t.
S (t): Number of susceptible nodes in the computer networks at time t.
E (t): Exposed class in the computer network at time t.
I_1 (t): Number of highly infected node in the computer network at time t.
I_2 (t): Number of low infected nodes in the computer networks at time t.
Q (t): The quarantine class mean infected computer seize for the shorts period of times at any instance t.
R (t): Number of recovery nodes in the computer networks at time t.
Λ : Rate at which new nodes attached to the computer networks.
μ : Nature death rate.
d : Rate of crash due to attack of malicious codes.

IoTP an Efficient Privacy Preserving Scheme for Internet of Things Environment

Shelendra Kumar Jainand Nishtha Kesswani (2020). *International Journal of Information Security and Privacy (pp. 116-142).*
www.irma-international.org/article/iotp-an-efficient-privacy-preserving-scheme-for-internet-of-things-environment/247430