Hindawi
Security and Communication Networks
Volume 2019, Article ID 6046353, 2 pages
https://doi.org/10.1155/2019/6046353

Editorial

Mathematical Models for Malware Propagation

Ángel Martín del Rey,[1] **Lu-Xing Yang**,[2] **and Vasileios A. Karyotis**[3]

[1] *University of Salamanca, Institute of Fundamental Physics and Mathematics, Department of Applied Mathematics, Salamanca 37007, Spain*
[2] *Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2600 GA Delft, Netherlands*
[3] *National Technical University of Athens, School of Electrical and Computer Engineering, Athens 157 80, Greece*

Correspondence should be addressed to Ángel Martín del Rey; delrey@usal.es

Received 19 December 2018; Accepted 20 December 2018; Published 2 January 2019

The dramatic increase of network services through the new paradigms such as cloud computing, Internet of Things, Industry 4.0, and critical infrastructures protection makes it necessary to develop tools and technologies to guarantee the security of digital data, processes, and networks against cyberattacks. These are becoming more and more sophisticated with the advent of advanced persistent threats.

Although the scientific approach to combat malware is mainly focused on the design of efficient methods to detect all types of malware, the design and computational implementation of mathematical models to simulate their spreading are also a very important task. These models allow us not only to predict the behavior of the evolution of malware, but also to study the efficacy of different possible countermeasures. As a consequence, these analytical tools could play a very important role in the forensic computing and cybercrime investigation as new techniques for the security operation centers.

The main goal of this special issue, which had opened for 8 months in the second half of 2017, is to investigate theoretical and practical aspects and design new applications in this research area.

Z.-H. Zhang et al. proposed a novel load capacity model against cascade failures considering clustering. The load redistribution strategy is a kind of nearest-neighbour redistribution methods, where the broken nodes allocate loads to their one-leap neighbours. Moreover, the strength of load redistribution proportion is governed by means of a tunable parameter. The model was simulated and analyzed on artificial and real networks of different type: ER random networks, BS scale-free networks, WS small-world networks, etc. These simulations suggested that networks with large average degree may be robust under the intentional attacks and highly clustered networks with the same degree distribution cannot guarantee the robustness.

Q. Zhu et al. introduced effective control strategies to control the virus spreading among computers and external devices using an optimal control approach: the external device blocking (that is, prohibiting a fraction of connections between external devices and computers) and computer reconstruction (including updating or reinstalling of some infected computers). Furthermore, this work took into account a state-based cost weight index in the objection functional instead of a fixed one and solved the problem by using Pontryagin's minimum principle and a numerical algorithm, respectively.

C. Zhang and J. Xiao proposed a novel dynamical model of an advanced persistent distributed denial-of-service attack (APDDoS) to analyze the behavior of an advanced persistent threat attack. It was a compartmental model where the devices are divided into weak-defensive computers (weak-defensive nodes and attacked devices) and strong-defensive computers (strong-defensive nodes and compromised nodes). The attacked threshold was derived and the global stability of the equilibrium points was studied.

Y. Yao et al. proposed a time-delayed worm propagation model considering variable infection rate. It was a compartmental model where susceptible, infectious, quarantined, vaccinated, and delay host were considered. The basic reproductive number was computed and a qualitative study was performed: the existence conditions and the stability of the unique positive equilibrium are derived by means of the

threshold of Hopf bifurcation. These results were numerically verified.

C. Zhang presented a computer virus propagation model on multilayer networks to understand the mechanism of computer virus spreading. It was a compartmental model where susceptible, latent, breaking out computers are considered. The author found out that the propagation threshold was the maximum eigenvalue of the sum of all the subnetworks on multilayer networks. The global stability of the virus-free equilibrium was studied and the persistence of the system was proved. These results were confirmed by means of extensive experiments.

Finally, P. Li et al. studied the effectiveness of advanced persistent threat (APT) defensive strategy which is quantified by considering a novel individual-level APT attack-defense model. Specifically, the APT defense problem was modeled as an optimal control problem and the existence of an optimal control was proven. The optimality system for the optimal control problem is derived. The influence of some factors on the effectiveness of an optimal control is analyzed through computer numerical simulations.

Conflicts of Interest

The editors declare that they have no conflicts of interest regarding the publication of this special issue.

Acknowledgments

We want to express our deepest gratitude to all authors for their excellent contributions and reviewers for their valuable help and suggestions. We also express our sincere thanks to the Editorial Board of SCN for their approval on this topic and their constant support in successful publication of this special issue. Finally, the Lead Guest Editor would like to show his great appreciation and to thank the two Guest Editors for their dedicated and excellent work.

Ángel Martín Del Rey
Lu-Xing Yang
Vasileios A. Karyotis