Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 433-437, 2016
ISSN 1990-9233;
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.TAET23420

Spreading Process Avoidance by Building Firewall in Base Station on Multilayer Networks

[1]*Ms. S. Kanmani and* [2]*Mr. K. Sankar*

[1]PG Scholar, Department of computer Science and Engineering,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India
[2]Asst. Prof, Department of computer Science and Engineering,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India

Abstract: Several systems can be modeled as sets of consistent networks or networks with multiple types of connections, here generally called multilayer networks. Spreading processes such as information proliferation among users of online social networks, or the diffusion of pathogens among persons through their contact network, are fundamental phenomenon occurring in these networks. However, while information diffusion in single networks has received considerable attention from various disciplines for over a decade, dispersion processes in multilayer networks is still a young research area present many challenging research issues. Firewall is been built in the base station of Multilayer Network while information will process through the base station and infected files are cleared. Spreading processes such as information broadcast among users of an online social networks, or the diffusion of pathogens among individuals through their contact network, are fundamental phenomenon occurring in these networks.

Key words: Multilayer network · Multiplex · Interconnected · Spreading processes · Information diffusion.

INTRODUCTION

For Personal Computer (PC) users, organizations and the military, Network security has become more important. With the advent of the internet, security became a major concern and the history of security allows a better perceptive of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the proper security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms.

Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of Switches. The internet is considered a data network. Since the current data network consists of computer based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers.

Multilayer networks have attracted interest again in recent years; the reader is referred to some recent review articles and books for general overviews of multilayer networks. Some of these works also contain discussions on spreading processes it is not intended to be a general review on multilayer networks; rather, here focus on spreading processes and therefore provide a more detailed coverage of this topic, also in terms of covered approaches, including a comprehensive categorization of models, applications and results that can help the reader to navigate the varied research landscape.

Evolution of Virus: System and network technologies are the significant technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical prerequisite in emerging networks, there is a significant

Corresponding Author: Ms. S. Kanmani, PG Scholar, Department of computer Science and Engineering,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India.

lack of protection methods that can be easily implemented. It contains several types of virus which are been affected into systems from the main source of the virus/malware from mainly internet and the filed which are been downloaded from the online social networks [1].

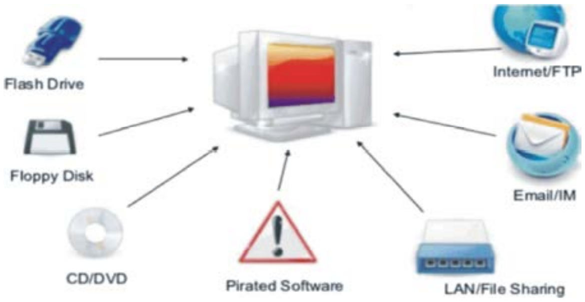

Fig. 1.1: Source of Malware

Network security starts with authenticating, commonly with a username and a password. Since this require just one detail authenticating the user name i.e., the password this is sometimes term one factor authentication. With two-factor authentication and with three-factor verification, something the user 'is' also used (e.g., a fingerprint or retinal scan).

Diffusion Process in Multilayer Networks: In many realistic systems, interconnections are so complicated that conventional simple networks cannot properly model the interconnections. Notions of multilayer and solid networks are among emerging topics in network science which go beyond conventional network representations. Multilayer networks are an abstract demonstration of interconnection among nodes representing individuals or agents, where the interconnection has a multiple nature.

Spreading Velocity: For example, while a disease can propagate among individuals during a physical contact network, information can propagate among the same individuals through an on-line information dissemination network. Another case in point is viral information dissemination among user of online social networks; one might disseminate information received from a Face book contact to followers in Twitter. Several open problems on these types of networks are due to their intrinsic complexity. Dynamics on a simple graph [2] usually depend on the spectral properties of its adjacency matrix. The Laplacian matrix, or some other graph-related matrices, which have been well studied and rigorously established, enable successful applications in practice.

Analyzing dynamics [3] on interconnected and multilayer networks is much more challenging. Researchers have formulated some problems in multilayer and interconnected networks which can be effectively analyzed through spectral properties of a bigger matrix.

Diffusion of Malware: Dynamical processes on these networks have become popular in recent years with diverse applications to cascading [4] failure diffusion synchronization and evolutionary games. In particular, the study of the spreading of epidemics in interconnected networks is a major challenge of complex networks [5], which has recently attracted substantial attention.

Spreading Process Avoidance: Information propagation is the spreading process among users of online social networks or the diffusion of pathogens among individuals through their contact network, are fundamental phenomena occurring in these networks. we focus on the practically relevant topic of spreading processes in multilayer networks a generic term that we use to refer to a number of models involving multiple networks, called interconnected networks.

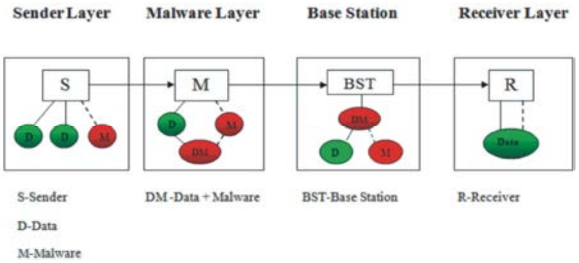

Fig. 2.1: Spreading Process Avoidance

Sender Layer transmits the information with the malware attached to the information file from sender to router layer which reads the corresponding information with the attached malware and then from the router layer information is transmit to the receiver layer and from the receiver layer the information is spread [6] out to their contacts of friends.

Epidemic Routing in Delay-Tolerant Networking (DTN): An epidemic model describes the spread of infections throughout a network. Susceptible-Infected-Susceptible (SIS) model is the model that describes about epidemics. In the SIS model, each node can be susceptible, become unhygienic with a given infection rate and become again susceptible with a given curing rate.

Epidemic Routing Algorithm: Add a new compartment to the classic SIS model to account for human response to epidemic spread [7]. Each individual can be infected, susceptible, or alert. Susceptible individuals can become alert with an alerting rate if infected individuals exist in their neighborhood.

An individual in the alert state is less probable to become infected than an individual in the susceptible state; due to a newly adopt cautious behavior.

Protocols based on encounter history, however, take time to build up a knowledge database from which to take routing decisions. While contact information changes regularly and it takes time to identify strong social ties, other types of ties remain rather stable and could be exploited to augment available partial contact information.

Flow of Pathogens in Multilayer Network

Generating Functions: Routing process in delay-tolerant networking distresses itself with the ability to transport, or route, data from a source to a destination, which is a fundamental ability all communication networks. Delay and disruption tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in a lack of instant end-to-end paths. In these challenging environments, popular ad hoc routing protocols such as AODV and DSR fail to establish routes.

This is due to these protocols annoying to first establish a complete route and then, after the route has been established, forward the actual data. However, when immediate end-to-end paths are difficult or impossible to establish, routing protocols must take to a "store and forward" approach.

The main models, results and applications of multilayer spreading processes and discuss some promising research commands practically relevant topic of spreading processes in multilayer networks is a generic term that is use to refer to a number of models involving several networks, called interconnected networks, or multiple types of relationships, called multiplex networks [8].

Malware Propagation: Information propagation is the spreading process among users of online social networks [9], or the diffusion of pathogens surrounded by individuals through their contact network, are fundamental phenomena occurring in these networks. focus on the practically appropriate topic of spreading processes in multilayer networks a generic term that we use to refer to a number of models involving multiple networks, called interconnected networks, or multiple types of relationships, called multiplex networks.

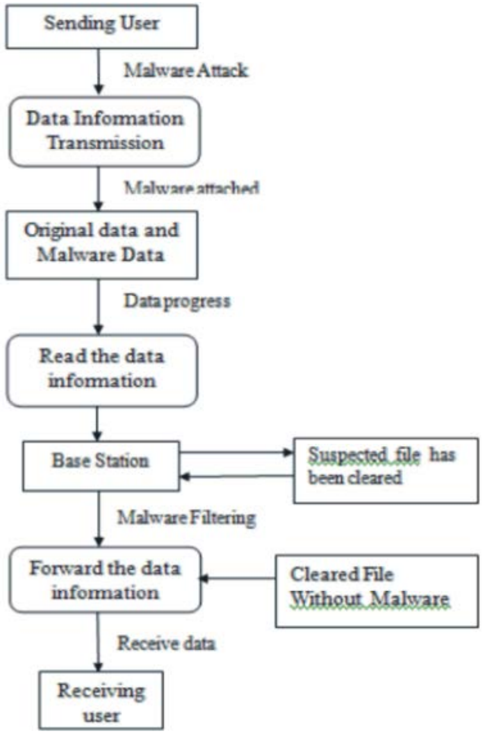
Sending User
Malware Attack
Data Information Transmission
Malware attached
Original data and Malware Data
Data progress
Read the data information
Base Station
Suspected file has been cleared
Malware Filtering
Forward the data information
Cleared File Without Malware
Receive data
Receiving user

Fig. 4.1: Process Flow of Pathogens Diffusion

Furthermore, recent work suggests that the epidemic threshold in a multiplex network cannot be larger than the epidemic thresholds of individual layers. In the context of interact spreading processes in multilayer networks, two types of thresholds have recently been introduced, called survival threshold and absolute-dominance threshold: they calculate if a spreading process will survive and whether it can completely remove another competing process.

Indeed, on one hand, information such as rumors, innovations and opinion diffuses through the underlying social networks. To whom and to how many people a user would pass such in sequence is constrained by whom s/he connect to and how well she is connected in the social network and the strength of those connections.

Signature Based Virus Detection: Signature based virus detection is the most common technique that is employed in traditional antivirus software [10] for identifying viruses. In this type of Antivirus software signature of some known virus calculated from the content of virus file and that signatures are store in the database of antivirus software.

Epidemic Propagation Filtering Layer: Base station contain firewall setting which is check the infection by virus if some infection or suspicion file found that will be repaired or delete the entire file. Signature based virus detection is the most common technique that is employed in traditional antivirus software for identifying viruses. In this type of Antivirus software signature of some known virus calculated from the content of virus file and that signatures are store in the database of antivirus software.

Pseudo-code for Signature Based Virus Detection

Step-1: Removable Drive Scan- When antivirus software scans for viruses and compare that signature with the signature present in the database.

Step-2: Startup Scan- To create a signature for virus.exe use the hash algorithms signature of virus. exe can be 48d4533230a1a1s118c741c0db19.

```
START: INSERT the Removable Disk
#process of scanning the Information
while scanning the information in Removable Disk do
    if file contain any Malware content then
        Compare the signature of Malware content with the signature of virus in database
    else
        There is no Infected File
    end if
    #process of scanning is completed
    return
end while
Open the files in Removable Disk.
```

Step-3: Scan with sample file- If signature of calculated file is match with the database present in the antivirus software at that time Antivirus software declare that file as a infected file and delete that particular file

CONCLUSION AND FUTURE WORK

Spreading processes in multilayer networks is an active and not yet consolidated research field and therefore offers many unsolved problems to address. In some cases, phenomena that are quite well understood in monopole networks are comparatively not well understood in the context of multilayer networks; in other cases, completely novel ideas, algorithms and analysis, specific to multilayer networks have to be developed.

To the best othere are no works based on real datasets on information diffusion [11] in multilayer networks and the whole of existing works on multilayer spreading are based on simulation or analytic studies. On the other hand, real-world multilayer networks are sometimes large and non-trivially observable.

ACKNOWLEDGMENT

This research was supported by my Head of the Department, Prof.T.R. Srinivasan. We grateful to thank Mr. Chandra Mohan for assistance with a technique and Mr. Sathish Kumar for comments that greatly improved the manuscript. We thank famous persons Dr. Karunanithi and Dr.K.C.K. Vijaykumar, for sharing their pearls of wisdom with us during the course of this research. And we thank Mr.K.Sankar and Mr.R.Rajagopal reviewers for their so-called insights. We are also immensely grateful to my family for their comments and support, although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

1. Gjoka, M. and C. Butts, 2011. “Multigraph sampling of online socialnetworks,” IEEE J. Sel. Areas Commun., 29(9): 1893-1905, Oct. 2011.
2. Buono, C., Alvarez-Zutuke and P. Macri, 2000. ”Network roburstness and Fragility:Percolation on random graphs”, pp: 4566, Dec-2000.
3. Nayak, A.K., A. Reimers, N. Feamster and R. Clark, 2009. “Resonance: Dynamic access control for enterprise networks,” in Proc. WREN, pp: 11-18.
4. Borge, G.J., S.N. Dorogovtsev and Y. Moreno, 2013. “Cascading behavior in complex social networks,” pp: 1, Apr.2013.
5. Gomez, S., A. Arenas and Y. Moreno, 2010. “Discrete-time Markov chain approach to contact-based disease spreading in complex networks,” EPL (Europhysics Lett.), 89(3).
6. Lin, Y. and C. Song, 2011. “Information spreading in context,” in Proc. 20th Int. Conf. World Wide Web, pp: 735-744.
7. Pastor-Satorras, R. and A. Vespignani, 2001. “Epidemic spreading in scale-free networks,” Phys. Rev. Lett., 86(14): 3200-3203, Apr. 2001.
8. Baxter, G.J., S.N. Dorogovtsev and D. Cellai, 2014. “Weak percolation on multiplex networks,” Phys. Rev. E, 89(4): 042801, Apr. 2014.
9. Qian, D., O. Yagan, L. Yang and J. Zhang, 2012. “Diffusion of real-time information in social-physical networks,” in Proc. IEEE GLOBECOM, pp: 2072-2077.

10. Mehdi, S.A., J. Khalid and S.A. Khayam, 2011. "Revisiting traffic anomaly detection using software defined networking," in Proc. RAID, pp: 161-180.
11. Bakshy, E., I. Rosenn, C. Marlow and L. Adamic, 2012. "The role of social networks in information diffusion," in Proc. 21st Int. Conf. World Wide Web, pp: 519-528.