SAJET

South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 130–135

**ISSN No: 2454-9614**

# Firewall Building in Base Station on Multilayer Network

S. Kanmani [a], K. Sankar [a*]

[a)] *Department Of Computer Science and Engineering, Vivekananda institute of engineering and technology for women, Tiruchengode , Tamilnadu, India.*
[b)] *Department Of Computer Science and Engineering, Vivekananda institute of engineering and technology for women, Tiruchengode,, Tamilnadu, India.*

*Corresponding Author: S. Kanmani

E-mail: Kanmanimecse@gmail.com,
**Received: 01/11/2015, Revised: 20/12/2015 and Accepted: 25/02/2016**

**Abstract**

Several systems can be modelled as sets of interconnected networks or networks with multiple types of connections, here generally called multilayer networks. Spreading processes such as information propagation among users of online social networks, or the diffusion of pathogens among individuals through their contact network, are fundamental phenomena occurring in these networks. However, while information diffusion in single networks has received considerable attention from various disciplines for over a decade, spreading processes in multilayer networks is still a young research area presenting many challenging research issues. The main models, results and applications of multilayer spreading processes and discuss some promising research directions. Spreading processes such as information propagation among users of an online social networks, or the diffusion of pathogens among individuals through their contact network, are fundamental phenomena occurring in these networks.

*Keywords: Multilayer network, multiplex, interconnected, spreading processes, information diffusion*.

**Reviewed by* **ICETSET'16** *organizing committee*

## 1. Introduction

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding 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 appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an “intranet” to remain connected to the internet but secured from possible threats.

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. 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. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e., the password this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis.

## 2. Spreading 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 interconnected networks are among emerging topics in network science which go beyond conventional network representations. Multilayer networks are an abstract representation of interconnection among nodes representing individuals or agents, where the interconnection has a multiple nature.

For example, while a disease can propagate among individuals through a physical contact network, information can propagate among the same individuals through an on-line information dissemination network. Another example is viral information dissemination among users of online social networks; one might disseminate information received from a Facebook contact to followers in Twitter.

Several open problems on these types of networks are due to their inherent complexity. Dynamics on a simple graph usually depend on the spectral property of its adjacency matrix, the Laplacian matrix, or other graph-related matrices, which have been well studied and strictly establish, enabling successful applications in practice.

Analyzing dynamics 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. In several large-scale systems, it is not possible to isolate a network completely: there are often many interconnections with one or more networks. Interconnected networks (abstract representations where two or more simple networks, possibly with different and separate dynamics upon them, are interconnected to each other. Dynamical processes on these networks have become popular in recent years with diverse applications to cascading 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, which has recently attracted substantial attention.

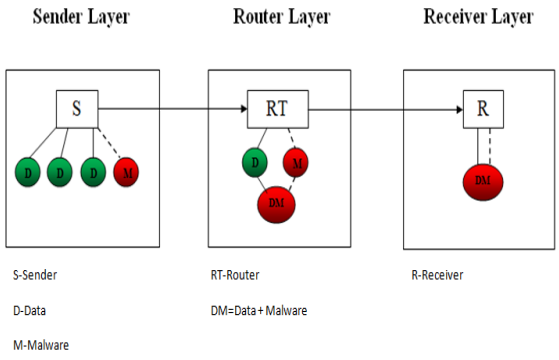


**Fig no: 2.1 Spreading Process**

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 been transmitted to the receiver layer and from the receiver layer the information is spread out to their contacts of friends and malware attached file is been transmitted to all other contacts and all files in the system will be affected by some type of malware which is been attached to the information that is transmitted from the sender to the receiver layer.

### 3. Epidemic Routing in Delay-Tolerant Networking (DTN)

An epidemic model describes how infections spread throughout a network. Among the compartmental models used to describe epidemics, the Susceptible-Infected-Susceptible (SIS) model has been widely used. In the SIS model, each node can be susceptible, become infected with a given infection rate, and become again susceptible with a given curing rate.

Add a new compartment to the classic SIS model to account for human response to epidemic spread. Each individual can be infected, susceptible, or alert. Susceptible individuals can become alert with an alerting rate if infected individuals exist in their neighbourhood. An individual in the alert state is less probable to become infected

than an individual in the susceptible state; due to a newly adopted cautious behaviour.

Protocols based on encounter history, however, take time to build up a knowledge database from which to take routing decisions. While contact information changes constantly 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.

**4. Diffusion of Pathogens in Multilayer Network**

Routing in delay-tolerant networking concerns itself with the ability to transport, or route, data from a source to a destination, which is a fundamental ability all communication networks must have. Delay and disruption tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in a lack of instantaneous 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 trying to first establish a complete route and then, after the route has been established, forward the actual data. However, when instantaneous 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 directions practically relevant topic of spreading processes in multilayer networks is a generic term that is use to refer to a number of models involving multiple networks, called interconnected networks ,or multiple types of relationships, called multiplex networks.

Spreading processes such as information propagation among users of online social networks, or the diffusion of pathogens among individuals through their contact network, are fundamental phenomena occurring in these networks. 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, or multiple types of relationships, called multiplex networks

Presenting the main dependent variables used in different spreading studies. The so-called epidemic threshold is one of the key observations in epidemic-like model and indicates a value of transmissibility above which the diffusion involves the whole (or most of the) network, e.g., the diffusion network is a giant component of the underlying network. It is known that in monoplex networks the value of the epidemic threshold is closely related to the largest Eigen value of the network's adjacency matrix.

Furthermore, recent work suggests that the epidemic threshold in a multiplex network cannot be larger than the epidemic thresholds of individual layers.

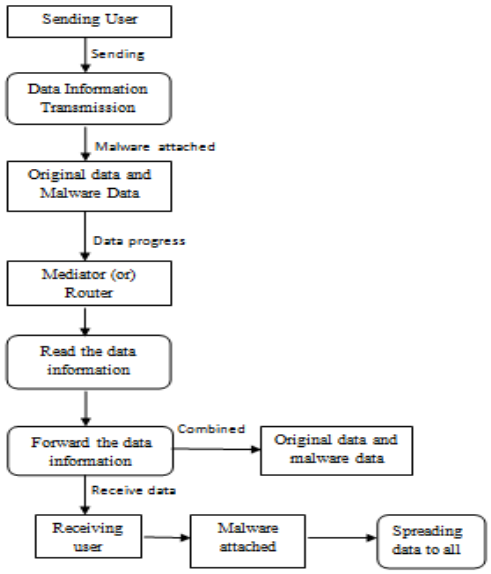


**Fig no: 4.1 Process Flow of Pathogens Diffusion**

In the context of interacting spreading processes in multilayer networks, two types of thresholds have recently been introduced, called survival threshold and absolute-dominance threshold: they measure if a spreading process will survive and whether it can completely remove another competing process.

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

## 5. 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 monoplex 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 of our knowledge there are no works based on real datasets on information diffusion in multilayer networks, and the totality 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, thus, it is worth exploring how different sampling approaches can impact the measurement of spreading processes here creating the pathogens detection in base station. If the sender sends the message to receive via the base station. The base stations scan the original message, divide and rectify the message and remove the pathogens and send the

original message. Outbreak detection is a technique for the detection of spreading of a virus (or information) in a network as quickly as possible.

## References

[1] Bakshy.E, Rosenn.I, Marlow.C, and Adamic.L, "The role of social networks in information diffusion," in Proc. 21st Int. Conf.World Wide Web, 2012, pp. 519–528.
[2] Baxter.G.J, Dorogovtsev.S.N, and Cellai.D,"Weak percolation on multiplex networks," Phys. Rev. E, vol. 89, no.4, p. 042801, Apr. 2014.
[3] Borge .G.J, Dorogovtsev.S.N, and Moreno.Y "Cascading behavior in complex social networks," vol. no,1,pp. Apr.2013
[4] Buono.C,Alvarez-Zutuke and Macri.P,"Network roburstness and Fragility:Percolation on random graphs", pp.4566,Dec-2000
[5] Callaway.D.S, Newman.M, and Watts. D.J "Network robustness and fragility: Percolation on random graphs," Phys. Rev. Lett., vol. 85, no. 25, pp. 5468–5471, Dec. 2000.
[6] Gjoka.M and Butts.C, "Multigraph sampling of online socialnetworks," IEEE J. Sel. Areas Commun., vol. 29, no. 9,pp. 1893–1905, Oct. 2011.
[7] Gomez.S, Arenas.A, and Moreno.Y,"Discrete-time Markov chain approach to contact-based disease spreading in complex networks," EPL (Europhysics Lett.), vol. 89, no. 3, Feb. 2010
[8] Lin.Y, Song.C, "Information spreading in context," in Proc. 20th Int. Conf. World Wide Web, 2011, pp. 735–744
[9] Pastor-Satorras.R and Vespignani.A,"Epidemic spreading in scale-free networks," Phys. Rev. Lett., vol. 86, no. 14, pp. 3200–3203, Apr. 2001.
[10] Qian.D, Yagan.O, Yang.L, and Zhang.J,"Diffusion of real-time information in social-physical networks," in Proc. IEEE GLOBECOM,2012, pp. 2072–2077.
[11] Van Mieghem.P,Omic.P, and Kooij.R, "Virus spread in networks," IEEE/ACM Trans. Netw., vol. 17, no. 1, pp. 1–14, Feb.2009.
[12] Wei.X, Valler.N, B. and Faloutsos.C, "Competing memes propagation on networks: a case study of composite networks," SIGCOMM Comput. Commun. Review, vol. 42, no. 5, pp. 5–12, Oct. 2012.