Dynamic Models on Prevention Mechanism of Attack In Computer Network

Partha Sarathi Chattaraj [a*]

[a] Department of CS,Yogoda Satsanga Mahavidyalaya,Ranchi,India.
*Corresponding author email id: partha75.in@gmail.com

ABSTRACT

This paper is to discuss the measures to be taken to secure the data from hackers and virus infection through dynamic security model. The paper is to explore the mechanism of protecting stored and online computer data and information from unauthorized use or modification. It concentrates on those hardware or software architectural structures that are necessary to support information protection. It uses several terms that involved and to solved for protecting data from unwanted threats. It also protects the system who is already connect within network then the system is activate their security model. If virus is present in the network, then first thing is to verify how many systems are already infected. It also includes verification of data, protection of data and prevention of data. This model is searching the network where hacking and virus may be possible and generated and search the system and group of system that are infected and may to infect others.

1. Introduction

Networks are backbone of any organization. The success of any organization largely depends upon their resource sharing between system to system in whole world through network. And in resource sharing, data are vital, for the any organization. So, security for protect the data and prevent from infection of virus, worms, hacking cracking is most important in the network and if any infection is raised then removed from the network is Also important. So, from the perspective of transmission mechanisms, mathematical models is very effective to protect and prevent from these type of threats and remove the infection of virus and protect from hacking on network and storage space. Mathematical model provides variety of factors like vector transmissions and also considered vertical, horizontal transmissions. Models integrate hatchingor dormant periods, confinements quarantines avoidance with assurance, or without information misfortune, and infection inside gatherings or between gatherings[1]. The organization elements of various kinds of organizations or gathering of organizations that scourge displaying bases on have been formed. The scourge model concentrated on additional confounded models with timedelays, mouddled structure, different code structure, or spatial construction[2]. Security relies upon huge number of ideas and conventions that can be utilized to guarantee protection where required. The main threats in the network is data hacking and virus attack on data and use them arithmetical model for detecting and removing the virus and worms attack and protect from hacking and cracking threats. These threats are main problem for a wireless and sensor network. In remote organization on the off chance that it is edited, made out of an enormous number of sensor hubs that are thickly conveyed inside the peculiarity or extremely close with one another[3-5]. In remote sensor network hubs need not fore ordained design or construction. This permits irregular arrangement in blocked off territories or catastrophe help tasks and which is vital benefit of this sort of organizations.Wireless sensor networks (WSNs)[6-8] have great potential for civil and military application and operation, that is why it is very much used in this field.

2. Literature review

Assessing the scope of a model, that is, less straight forwarding to determining what situation the model is applicable If the model was constructed based for "typical" set of data then must determine which system or situation is used for that. The question of whether the model describes well the properties of the system or group of system between and outside the observed data points like interpolation and extrapolation.

3.Methodology and tools

3.1 Epidemiological modelling:

The term epidemiological displaying alludes to the powerful demonstrating process where the complete organizations is partitioned into a specific convention for exchange of information characterized by internet or client characterized and classes-based network[9-17]. So, it is vital to be familiar with their epidemiological status and afterward differential or contrast conditions are utilized to address the developments of information between the compartment of framework and gatherings of framework through network on account of reasons like infection, hacking, breaking, insurance, avoidance and recuperation, and so on. To form a powerful model for the transmission impact of pestilence in framework and in given network then it is important to partition into a few unique gathering or compartments of organizations in the middle between framework. Such a model depicting the powerful relation among these compartments is known as a framework compartment model. The steps of compartmental ordinary differential equations

models are as follows:
Assume the contamination is partitioned into n sickness stages, or compartments.

1. Let x (t) be the vector of populaces in each stage.
2. Accept the all-out populace is huge, and that the absolute number of tainted people islittle, so we might expect the quantity of defenseless has generally consistent.
3. $x'(t) = F\,x(t) - V\,x(t)$,
4. The (i, j) passage of the change network V is the rate, people in stage j progress toorganize I.
5. The (i, j) entry of transition matrix F is the number of new infections at stage j, caused bycontacts with diseased individuals in stage i.

Dynamic models for irresistible sicknesses or PC worms/infections are generally founded on compartment structures that were at first proposed by Kermack and McKendrick (1927, 1932) and grew later by numerous different mathematicians[18-19].
The *Susceptible* (S) class includes those units of the networks or groups of networks which are free from virus infection i.e. they are healthy but they have an active potential threat of infection by the infective network at any point of time.
The Class of Uncovered (E) class incorporates the asymptomatic idly tainted units of the organizations or organizations bunches who have been in touch with the infection specialist however are yet to show any infective consequences for the leftover segment of the organizations. The Irresistible (I) class incorporates the units that have been infection tainted and who presentlycan possibly send the irresistible sickness to the other organizations or gatherings of organizationon having satisfactory contacts with the vulnerable class of the organizations.
The Recovered or Eliminated (R) class incorporates those singular arrangement of gatherings who have quit being irresistible and have procured counteraction and security, which might be long-lasting or brief in view of whether they stay in this class always or they move back to the vulnerable class and consequently they quit being irresistible to different units. The Protected (P)network is to check each unknown and individual system for detect the virus, hacker and crackers and also files which comes through network. If virus is checked then the network can block that individual removed the virus. The Infectivity Contact Rate might be characterized as the normal number of sufficient contacts for example the contacts adequate for transmission of contamination per PC hub per unit time. Assume N is the all-out number of PC hubs and β is the pace of transmission of worms from class S to class E/I, then infectivity contact rate can be taken as, $(\beta N)(S/N)I = \beta SI$. The Essential Propagation Number R0 (otherwise called Edge Boundary)is really the normal number of optional contaminations created by one tainted person during the mean course of disease in a totally defenseless populace. The idea of limits lays out the basics of

the hypothesis of plague elements. For computational purposes, R0 = (Pace of optional contamination) × (length of disease)

There are some aspects of this number to explore:

Structure of the host network

- Virus
- Behavior of virus
- Treatment of virus
- Type of multiple networks (vector host)
- Heterogeneities in space

1. Dynamics of the virus-free networks

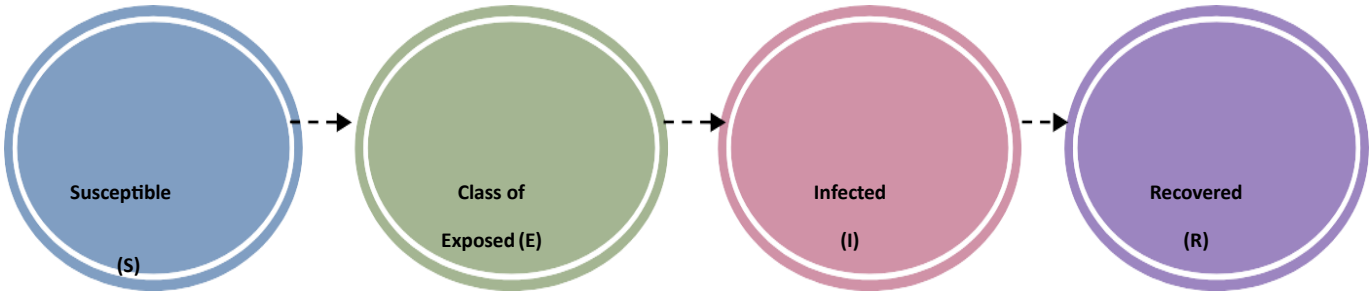
3.2 simple epidemic models

A straightforward old style SIR (Vulnerable, Irresistible, Recuperated) model portrays the elements of straightforwardly sent worms/infection with cooperation among helpless, tainted andrecuperated hubs in the PC organization. The schematic chart for the progression of worms/infection in PC organization (figure 1) model can be addressed as:

Where β is the rate of contact and α is the rate of transmission of worms from class *I* to class *R*.In this model, the flow of worms is from class *S* to class *I* and class *I* to class *R*. The basic reproduction number R_0 for this model is,

$R_0 = \beta / \alpha$. The Class of Exposed which exposed the class that will maybe infected through infection.

To get (SEIR) (Vulnerable, Class of Uncovered, Irresistible, Recuperated) model, we just add uncovered class E (withε, which is rate of transmission from class *E* to class *I*) in SIR model. The schematic diagram for the flow of worms in computer network (figure 2) model can be represented as:



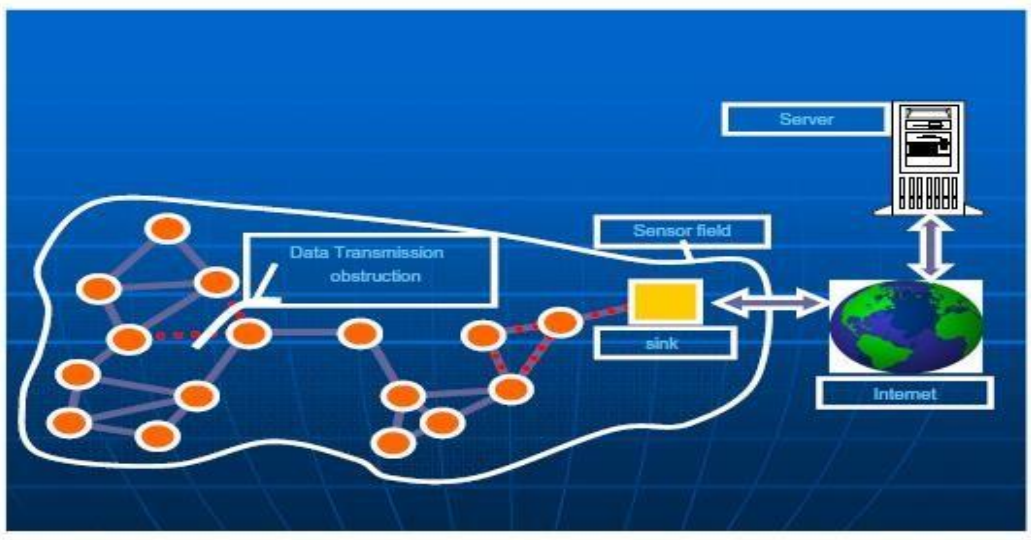


Fig. 1. Sensor network communication structure.

3.3 Simple epidemic models

Early trailblazers in irresistible sickness displaying were William Hamer and Ronald Ross, who in the mid 20th century applied the law of mass activity to make sense of scourge conduct. Lowell Reed and Swim Hampton Ice fostered the Reed-Ice pandemic model to portray the connection between helpless, tainted and resistant people in a populace.

3.4 CONCEPTS

*R*0, The basic reproduction number. The average number of other individuals nodes each infected, individual nodes will infect in a total population of nodes in the network that has no immunity from virus, worms etc.

S The proportion of the population of nodes who are susceptible to the virus or different typesof attacks (neither immune nor infected).

A The average nodes at which the disease (virus or worms etc.) is contracted in a given population of nodes. *L* The average life expectancy in a given population of nodes.

4 .Conclusion

This research work is to define the behavior of attack and threats in computer network and groups of network and also the prevention or protection from virus, worms, hacking and cracking. After the study the conclude that if we want to know about the nature of virus and theirexpandability rate in the network which may be infrastructural architecture, wireless or sensor network then to stop this type of threats, using mathematical formula, network can detect that type of threats and security can spread through dynamic architectural model. Our main motive is to stop this type of threats in early stage. At the point when need to identify the spreading worms then initially comprehend what worms proliferate and how unique examining methodologies mean for worm engendering elements. In this examination works, we efficiently model and break down worm engendering under different checking techniques.

Reference

1. S. Tang, W. Li, (2006) Qos supporting and optimal energy allocation for a cluster-based wirelesssensor network, Comput. Commun. 29, 2569–2577.
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications magazine, 40(8), 102-114.S.Stantiford, V. Paxton, Weaver, in: Proc. Of the 11th USENIX Security Symposium(Security '02), 2000.
3. Chen, T. M., & Robert, J. M. (2004). Worm epidemics in high-speed networks. Computer, 37(6), 48-53.
4. Pastor-Satorras, R., & Vespignani, A. (2004). Evolution and structure of the Internet: A statistical physics approach. Cambridge University Press.
5. Nekovee, M. (2007). Worm epidemics in wireless ad hoc networks. New Journal of Physics, 9(6), 189.
6. Szor, P. (2005). Art of Computer Virus Research and Defense, The, Portable Documents. Pearson Education.
7. Dagon, D., Martin, T., & Starner, T. (2004). Mobile phones as computing devices: The viruses are coming!. IEEE Pervasive Computing, 3(4), 11-15.
8. Chien, E. (2005). Security response: Symbos. mabir. Symantec Corporation, 10, 108.
9. Mishra, B. K., & Saini, D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied mathematics and computation, 188(2), 1476-1482.
10. Mishra, B. K., & Saini, D. (2007). Mathematical models on computer viruses. Applied Mathematics and Computation, 187(2), 929-936.
11. Mishra, B. K., & Jha, N. (2007). Fixed period of temporary immunity after run of anti-malicious software on computer nodes. Applied Mathematics and Computation, 190(2), 1207-1212.
12. Gelenbe, E. (2007). Dealing with software viruses: a biological paradigm. information security technical report, 12(4), 242-

250.
13. Çaglayan, M. U. (2015). ISCIS and Erol Gelenbe's Contributions. In Information Sciences and Systems 2015: 30th International Symposium on Computer and Information Sciences (ISCIS 2015) (pp. 3-17). Cham: Springer International Publishing.
14. Gelenbe, E., Kaptan, V., & Wang, Y. (2004). Biological metaphors for agent behavior. In International symposium on computer and information sciences (pp. 667-675). Berlin, Heidelberg: Springer Berlin Heidelberg.
15. Mishra, B. K., & Keshri, N. (2013). Mathematical model on the transmission of worms in wireless sensor network. Applied Mathematical Modelling, 37(6), 4103-4111.
16. Piqueira, J. R. C., Navarro, B. F., & Monteiro, L. H. A. (2005). Epidemiological models applied to viruses in computer networks. Journal of Computer Science, 1(1), 31-34.
17. Forrest, S., Perelson, A. S., Allen, L., & Cherukuri, R. (1994). Self-nonself discrimination in a computer. In Proceedings of 1994 IEEE computer society symposium on research in security and privacy (pp. 202-212). Ieee.
18. Wang, Y., & Wang, C. (2003). Modeling the effects of timing parameters on virus propagation. In Proceedings of the 2003 ACM workshop on Rapid Malcode (pp. 61-66).
19. Dietz, K. (1997). Introduction to McKendrick (1926) Applications of mathematics to medical problems.

Received 09 November 2023
Revised 29 January 2024
Accepted 11 March 2024