International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

THE HIDDEN VIRUS PROPAGATION SEARCH ENGINE ATTACK

Aswini.V[1], Meena.S[2], Vinmathi .M.S[3]

[1,2] *Student Member, Dept. of CSE, Panimalar Engineering college, Tamil Nadu, India*
[3]*Associate Professor, Dept. of CSE, Panimalar Engineering college, Tamil Nadu, India*

Abstract - *Many real-world networks exhibit overlapping community structure in which vertices may belong to more than one community. We classify vertices into overlapping and non-overlapping ones, and investigate in detail how they affect epidemic spreading respectively. One of the important dynamics on complex networks is epidemic spreading. An important issue is, for a given community structure of complex network, how the infection propagates and whether there exist effective control strategies for preventing or suppressing the spread of infection. When an epidemic spreads in a population, individuals may adaptively change the structure of their social contact network to reduce risk of infection. Here we study the spread of an epidemic on an adaptive network with community structure. In a static network, weakly connected heterogeneous communities can have significantly different infection levels. In contrast, adaptation promotes similar infection levels and alters the network structure so that communities have more similar average degrees.*

Key Words: ***Epidemic spreading***, ***infection propagation***, ***infection level, average degree***.

1. INTRODUCTION

The current research on network virus propagation can be divided into two categories: some researchers model the propagation of virus to find the threshold of a large-scale breakout, while others attempt to study the mechanism of a restraining virus. In the study of virus defense in the mobile network, it is found that virus propagation in a mobile network is difficult to restrain because the topology of the network is changing frequently due to the mobility of devices. There are two kinds of strategies restraining the virus in a mobile network: immunization strategy and local strategy. In most cases, immunization strategies are implemented based on centralized distribution and static network. Within a group, each member is directly connected to most other members, but connections among different groups are relatively rare. In some degree, structure determines the characteristics and function of networks. To explain the mechanism of social networks, several models have been presented, which include the mutual friendship approach, dense links in community and sparse links between communities. Computer worms, which have been rampant in the Internet for more than two decades, are nothing new to us. Bluetooth worms significantly differ from Internet worms in three ways. First, the limited transmission range of a Bluetooth device leads to a proximity-based infection mechanism: a Bluetooth-enabled device controlled by the worm can only infect neighbors within its radio range. This differs from Internet worms that often scan the entire IP address space for susceptible victims. Second, the bandwidth available to Bluetooth devices is usually much narrower than those of Internet links. For instance, the maximum transmission rate of a device operating on the class 2 Bluetooth radio is 1 Mbps. The input parameters fed to this model include some key statistical metrics that describe the underlying mobility patterns, such as average node degree, average node meeting rate, and the link duration distribution. The input parameters of the model also include control parameters used by the Bluetooth worms, such as how much time the Bluetooth worm spends at most on discovering new victims and how many victims it expects to discover within a single infection cycle, and how long the Bluetooth worm remains dormant before it is activated again for new infection attempts.

Problem Definition

In the traditional view, viruses cannot spread among unconnected nodes or communities. But in fact, virus propagation can occur among global users or communities in social networks through search engines, regardless of the connectivity of nodes and communities. We call this phenomenon the propagation wormhole effect. The propagation wormhole effect is the specific manifestation of the hidden power of search engines on virus propagation. A primary challenge for analysing the virus propagation effect of search engines lies in figuring out the processes by which a search engine increases the number of infection sources and the infection routes. Emotion categories, namely, awe, amusement, contentment excitement, anger, disgust, sadness, fear and boredom. Then, we investigate whether user demographics such as gender, marital status and occupation are related to the emotional tags of social images. We uncover several patterns, and a partially labelled factor graph model named the demographics factor graph model (D-FGM) is proposed to leverage user demographics in the modelling as different factors.

Architecture Diagram

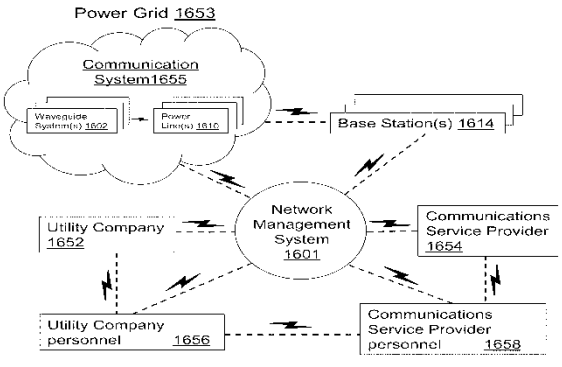


FIG. 16B

MODULES:

SEARCH ENGINE MODULE

In this module the user login to the application and use search engine to search any content of data in the application to get the required data with respective to the keywords entered in the search engine.

UNOFFICIAL URL BLINK MODULE

The user click the unofficial links and get access the data along with virus which get affected along with the retrieval of data then application sends the notification to the admin for the virus detection.

VIRUS PROPAGATION ANALYSATION MODULE

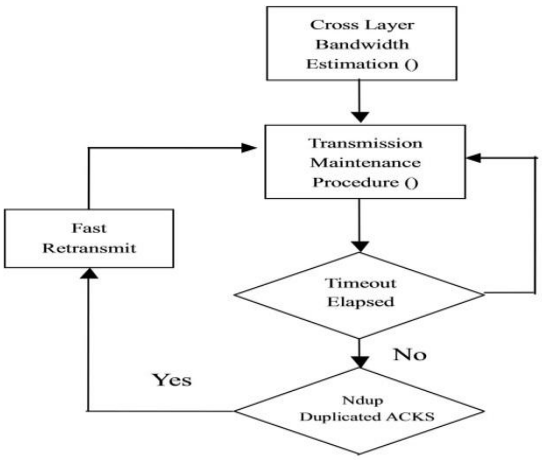
Admin analysis the gets details of malicious virus and uses search engine to analysis the path of virus to analysis the propagation of virus content in each nodes and analysis percentage of affected nodes at each path.

FEEDBACK MODEL WITH TIME DELAY

Overview of Time Delay

In a communications system, propagation delay refers to the time lag between the departure of a signal from the source and the arrival of the signal at the destination. This can range from a few nanoseconds or microseconds in local area networks (LANs) up to about 0.25 s in geostationary-satellite communications systems. Additional propagation delays can occur as a result of the time required for packets to make their way through land-based cables and nodes of the Internet. Hold time is also a timing parameter associated with Flip Flops and all other sequential devices. The Hold time is used to further satisfy the minimum pulse width requirement for the first (Master) latch that makes up a flip flop. The input must not change until enough time has passed after the clock tick to guarantee the master latch is fully disabled. More simply, hold time is the amount of time that an input signal (to a sequential device) must be stable (unchanging) after the clock tick in order to guarantee minimum pulse width and thus avoid possible met stability. Propagation delay of a logic gate is defined as the time it takes for the effect of change in input to be visible at the output. In other words, propagation delay is the time required for the input to be propagated to the output. Normally, it is defined as the difference between the times when the transitioning input reaches 50% of its final value to the time when the output reaches 50% of the final value showing the effect of input change. Here, 50% is the defined as the logic threshold where output (or, in particular, any signal) is assumed to switch its states. Liberty file contains a lookup table for the each input-to-output path (also called as cell arc) for logic gates as .lib models. The table contains values for different input transition times and output loads corresponding to cell delay. Depending upon the input transition and output load that is present in the design for the logic gate under consideration, physical design tools interpolate between these values and calculate the cell delay.

FLOWCHART



RELATED WORKS

There are several important parameters in our model for the derivation of the infection rate _ that require careful evaluation for the propagation model to achieve the desired accuracy. For MICA2 motes, the maximum packet transmission rate is around 36 packets/second with a packet size of 32 bytes. This results in a packet transmission time of 0.027 second. The average packet loss rate due to effects such as packet collisions, etc., is assumed to lie between 0.1 and 0.2 which is the average value derived from simulation data. Thus, in our formulation, l ¼ 0:1 and Tpkt ¼ 0:027 second. Simulation results of Deluge [11] have shown that the average number of requests for acquiring a page E½Nreq_ is approximately equal to 5.4.Our simulation works in two phases. In the first phase, we form the network where each node identifies its set of neighbors and entries are made into a neighbor table. By randomly choosing links to keep or delete, we control the average degree of the

network. We perform this by modifying the transmit power of individual nodes so as to change the average number of total links in the network. The entry for each node in the neighborhood table can indicate whether a node is susceptible, infected, or recovered. We outline the simulation setup and detail to implement the propagation process in each of the three broadcast protocols. The time dynamics of the malware spread is captured with varying degrees of infectivity on the whole network. We have used JProwler [4], a probabilistic, event-driven wireless network simulator in Java, for our experiments.

CONCLUSION

With the proliferation of social networks and their ever increasing use, viruses have become much more prevalent. We investigate the propagation effect of search engines, and characterize the positive feedback effect and the propagation wormhole effect. The virtual virus pool and virtual infection paths that are formed by a search engine make propagation take place much more quickly. We show that propagation velocity is quicker, infection density is larger, the epidemic threshold is lower and the basic reproduction number is greater in the presence of a search engine. Finally, we conduct experiments that verify the propagation effect in terms of both infection density and virus propagation velocity. Results show the significant influence of a search engine particularly its ability to accelerate virus propagation in social networks.

Broadcast protocols in sensor networks are vulnerable as potential carriers of malwares/viruses that spread over air interfaces. In this paper, we have provided a common mathematical model to analyze the process of malware propagation over different multichip broadcast protocols, although approximately, our model successfully captures the ripple-based propagation behavior of the wave front of a broadcast protocol. Not only is the model capable of assessing the performance of each protocol in the face of a virus outbreak, but it also helps in comparing their vulnerabilities against each other. Its generic and flexible nature allows us to conveniently fit parameters of different broadcast protocols and analyze their susceptibilities. Despite the similarities in operation between some of the protocols discussed, the epidemic model successfully highlights their differences from a propagation standpoint.

REFERENCE

[1] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, W. Jia, and C. C. Zou, "Modeling and analysis on the propagation dynamics of modern email malware," IEEE Trans. Dependable Sec. Computer., vol. 11, no. 4, pp. 361–374, 2014.

[2]J. Zhang and Z. Jin, "Epidemic spreading on complex networks with community structure," Applied Mathematics and Computation, vol. 219, no. 6, pp. 2829–2838, 2012.

[3] C. Fu, Q. Huang, L. Han, L. Shen, and X. Liu, "Virus propagation power of the dynamic network," EURASIP J. Wireless Comm. AndNetworking, vol. 2013, p. 210, 2013.

[4] L. Lu, R. Perdisci, and W. Lee, "SURF: detecting and measuringsearch poisoning," in Proceedings of the 18th ACM Conference onComputer and Communications Security, CCS, Chicago, Illinois, USA,October 17-21, 2011, pp. 467 476.

[5] H. W. S. Herbert W. Hethcote and P. V. D. Driessche, "Nonlinearoscillations in epidemic models," Society for Industrial and AppliedMathematics, vol. 40, no. 1, pp. 1 9, 2006.

[6] Y. Zhou and X. Jiang, "Dissecting android malware: Characterizationand evolution," in IEEE Symposium on Security and Privacy,SP, 21-23 May, San Francisco, California, USA, 2012, pp. 95–109.

[7] K. Aoki, T. Yagi, M. Iwamura, and M. Itoh, "Controlling malwareHTTP communications in dynamic analysis system using search engine," in CSS, 2011, pp. 1–6

[8] J. Shang, L. Liu, F. Xie, and C. Wu, "How overlapping community structure affects epidemic spreading in complex networks," in IEEE 38th Annual Computer Software and Applications Conference,COMPSAC Workshops, Vasteras, Sweden, July 21-25, 2014, pp. 240– 245.

[9] I. Tunc and L. B. Shaw, "Effects of community structure on epidemic spread in an adaptive network," CoRR, vol. abs/1212.3229, 2012.

[10] J. T. Jackson and S. Creese, "Virus propagation in heterogeneous Bluetooth networks with human behaviors," IEEE Trans. Dependable Sec. Comput., vol. 9, no. 6, pp. 930–943, 2012.