DYNAMICS OF MALWARE SPREAD IN DECENTRALIZED PEER-TO-PEER NETWORK

Tanmayi Mhatre*

Dipali Shinde*

Saili Budbadkar*

ABSTRACT

Malware is the software developed with malicious intentions. The detection of such malware can be done by writing program which can understand the dynamics of malware. This paper presents an analytical model which can effectively characterize the true nature of malware and how it spreads in peer-to-peer networks such as Gnutella. The proposed model is compartmental model which involves derivation of network conditions and system parameters in such a way that under those parameters and conditions the underlying P2P network reaches a malware free equilibrium. The proposed model can also perform evaluation of strategies such as quarantine used to control malware spread. Afterwards the model has been enhanced and tested with networks of smart cell phones.

Keywords— Malware, Peer to Peer Decentralized Network.

* Department Of Information Technology, Padmabhushan Vasantdada Patil Pratisthans College Of Engineering, Mumbai.

1. INTRODUCTION

The use of peer-to-peer (P2P) networks as a vehicle to spread malware offers some important advantages over worms that spread by scanning for vulnerable hosts. This is primarily due to the methodology employed by the peers to search for content. For instance, in decentralized P2P architectures such as Gnutella where search is done by flooding the network, a peer forwards the query to its immediate neighbours and the process is repeated until a specified threshold time-to-live, TTL, is reached. Here TTL is the threshold representing the number of overlay links that a search query travels. A relevant example here is the Mandragore worm that affected Gnutella users.

The design of the search technique has the following implications: first, the worms can spread much faster, since they do not have to probe for susceptible hosts and second, the rate of failed connections is less. Thus, rapid proliferation of malware can pose a serious security threat to the functioning of P2P networks. Understanding the factors affecting the malware spread can help facilitate network designs that are resilient to attacks, ensuring protection of the networking infrastructure. This project addresses this issue and develops an analytic framework for modelling the spread of malware in P2P networks while accounting for the architectural, topological, and user related factors. We also model the impact of malware control strategies like node quarantine.

2. REVIEW OF LITERATURE

A. EXISTING SYSTEM:

Previous simulation model uses a combination of the Epidemiological model and a Empirical model to model the effect of large-scale worm attacks.

In an Existing system the complexity of the Empirical model makes it difficult to derive insightful results that could be used to contain the worm.

In a previous study it is used to detect the presence of a worm by detecting the trend, not the rate, of the observed illegitimate scan traffic.

The filter is used to separate worm traffic from background non worm scan traffic.

B. DISADVANTAGES OF EXISTING SYSTEM:

a. Assumptions in Epidemiological mode

Epidemiological models to study malware spread in P2P networks. These studies assume that a vulnerable peer can be infected by any of the infected peers in the network. This assumption is invalid since the candidates for infecting a peer are limited to those within TTL hops away from it and not the entire network. Another important omission is the incorporation of user behavior. Typically, users in a P2P network alternate between two states: the on state, where they are connected to other peers and partake in network activities and the off state wherein they are disconnected from the network. Peers going offline result in fewer candidates for infection thereby lowering the intensity of malware spread.

b. Empirical model ignores node dynamics

An empirical model for malware spreading in BitTorrent is developed in while models for the number of infected nodes by dynamic hit list-based malware in BitTorrent networks is presented . However, these models ignore node dynamics such as online-offline transitions and are applicable only to BitTorrent networks. the authors use hypercube as the graph model for P2P networks and derive a limiting condition on the spectral radius of the adjacency graph, for a virus/worm to be prevalent in the network. The models do not account for the fact that once a peer is infected, any susceptible peer within a TTL hop radius becomes a likely candidate for a virus attack.

c. PROPOSED SYSTEM:

Proposed model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage.

We obtain the probability that the total number of hosts that the worm infects is below a certain level.

Our strategy can effectively contain both fast scan worms and slow scan worms without knowing the worm signature in advance or needing to explicitly detect the worm.

Our automatic worm containment schemes effectively contain the worms and stop its spreading.

In proposed system we are going to generate the graph containing information about both the active and inactive nodes.

This node information will allow us to keep track of all nodes in TTL hops. Thus allowing us to identify infected nodes which are in active or inactive state.

d. COMPARISON WITH EXISTING SYSTEM:

1. Proposed system is more secured and accurate in comparison to existing system:-

The proposed system is more secure in comparison to existing system.It helps in better way to prevent and stop the attacks from the worms.The multiple scanning options helps the system to function in a better way.

2. Proposed system is less complex than the existing system:

The existing system uses a combination of the deterministic epidemic model and a general stochastic epidemic model to model the effect of large-scale worm attacks.In an Existing system the complexity of the general stochastic epidemic model makes it difficult to derive insightful results that could be used to contain the worm.The proposed model uses the automatic worm containment model.

3. Proposed system works more faster than the existing system:

The proposed model contains effectively contain both fast scan worms and slow scan worms without knowing the worm signature in advanced or needing to explicitly detect the worm.

3. SYSTEM ARCHITECTURE:

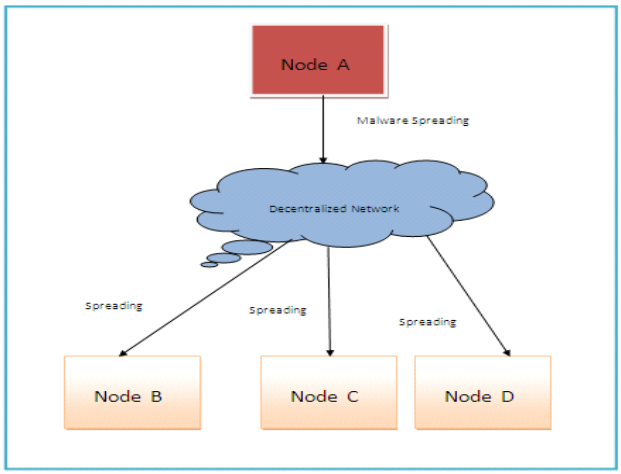

Figure .1:System Architecture

As Shown in the Figure1,

The architecture of DYNAMICS OF MALWARE SPREAD IN DECENTRALIZED PEER-TO-PEER NETWORK is based on decentralized peer to peer network

The system consists of 5 main modules .The main modules are:

A. User Interface Design

In this module we have designed the user interface for all the hosts. We design the user interface to show our propagation of worms in a graphical manner or GUI. By showing the output in GUI gives more attractive and understandable to everyone. Then we design the containment window to show the scanning, detection of worms. Thus we design the whole user interface in this module.

B. Worm Propagation Model

In this module, we create a worm spreading model. This model is designed for the propagation of worms inside a network. Inside the network we spread the worms in a controlled environment. To create worm propagation model we need to form a network by using the server socket class and socket class available in Java. These two classes are used to create a connection to transfer data from a host to other host inside a network.

C. Scanning for worms

Our strategy is based on limiting the number of scans to dark-address space. The limiting value is determined by our analysis. Our automatic worm containment schemes effectively contain both uniform scanning worms and local preference scanning worms, and it is validated through simulations and real trace data to be non-intrusive.

D. Detecting and categorizing worms

The model is developed for uniform scanning worms and then extended to preference scanning worms. We detect these two worms and categorize it in this module.

E. Containment of worms

This model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, we are able to 1) provide a precise condition that determines whether the worm spread will eventually stop and 2) obtain the distribution of the total number of hosts that the worm infects.

4. TECHNOLOGY AND CONCEPTS:

The following depicts the concepts and technology used in the proposed system.

A. AUTOMATIC WORM CONTAINMENT STRATERGY:

Automatic worm containment strategy prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, it is able to 1) provide a precise condition that determines whether the worm spread will eventually stop and 2) obtain the distribution of the total number of hosts that the worm infects.

B. WORM TRAFFIC:

Worm Traffic is nothing but the traffic created due to the rapid proliferation and spreading of the worms on the network.Such network traffics may damage the functioning and thus may damage the overall system**.**

5. IMPLEMENTATION

For the development of the proposed system we have used Java and database whish is accomplished with Sql.

We have developed the GUI using java which are as follow:

Node A:

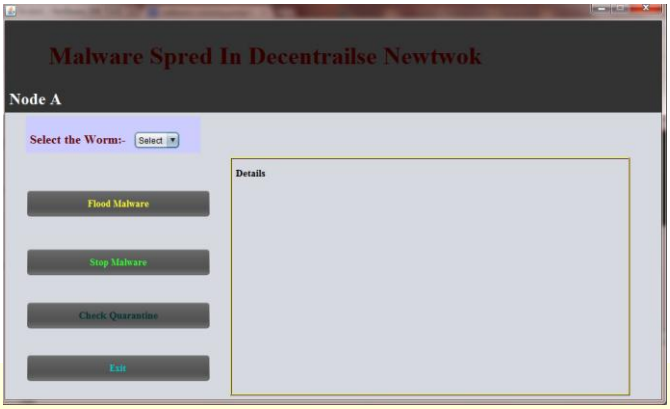

Fig.2 Node A

Node B:

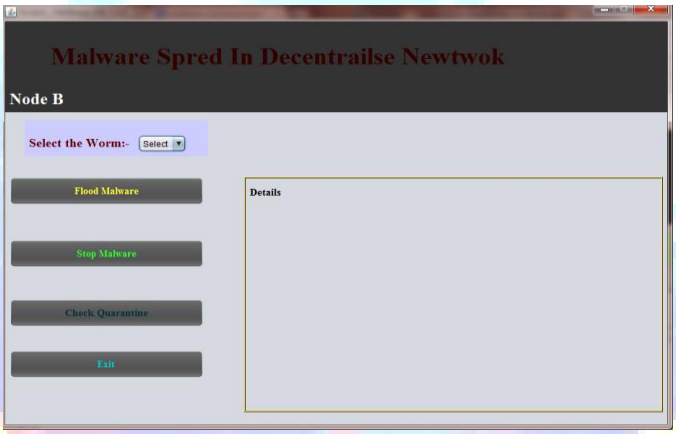

Fig.3 Node B

As shown in above GUI system will spread malware in network using 'flood malware' option .The spread of malware can be controlled by using 'stop malware' option on GUI.

For detecting the malware during data transfer we have given the option 'check quarantine' which will scan the packets coming to any node. And delete the contaminated packets.

The detailed information about data transfer can be seen in 'details' window where the system will provide information about following:

1) Total packets transferred
2) Source node of received data
3) Total no. of contaminated packets
4) Total no. of packets discarded.

6. CONCLUSION

Dynamics of malware spread in decentralized peer to peer network is thus a system providing security for data transmission and communication in decentralized peer to peer network. It also provides security to devices in network against malware attack.

The proposed system will provide the detailed information about states of devices in network, whether they are infected or not.

Proposed system will provide the status of data transfer in terms of total packets transferred, no. of infected packets and information about the node from which the infected data arrived at destination node.

Thus providing detailed information about nodes in network which will help for future data transfer in network.

ACKNOWLEDGEMENT

We are grateful to this institute for having channelized our skills and energy and for encouraging us to work together with cooperation and co-ordination. We are indebted to our inspiring HEAD OF DEPARTMENT and Internal Project Guide MRS.PRACHI KSHIRSAGAR and also our Principal Dr.K.T.V REDDY who have extended all valuable guidance, help and constant encouragement through the various difficult stages in the development of the project.

REFERENCES

[1] Krishna ,Ramachandran and BiplabSikdar,"Dynamics of Malware Spread in Decentralized Peer-to-Peer Networks", IEEE Transactions on Dependable and Secure Computing, Vol. 8, No.4, July/August 2011.

[2] Andrew Kalafut, Abhinav Acharya, Minaxi Gupta, "A Study of Malware in Peer-to-peer Networks".

[3] "Anticipation Measures For Protecting P2P Networks From Malware Spread", The International Journal of Engineering And Science(Ijes) Vol.2, Issue-2,2013

[4] BOOK: Complete Reference JAVA.

[5] X. Yang and G. de Veciana, "Service Capacity in Peer-to-Peer Networks," Proc. IEEE INFOCOM '04, pp. 1-11, Mar. 2004.

[6] J. Mundinger, R. Weber, and G. Weiss, "Optimal Scheduling of Peer-to-PeerFile Dissemination," J. Scheduling, vol. 11, pp. 105-120, 2007.

[7] A. Bose and K. Shin, "On Capturing Malware Dynamics in Mobile Power-Law Networks," Proc. ACM Int'l Conf. Security and Privacy in Comm.Networks (SecureComm), pp. 1-10, Sept. 2008.

[8] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa, and S. Chien, "AFirst Look at Peer-to-Peer Worms: Threats and Defenses," Int'l WorkshopPeer-To-Peer Systems, Feb. 2005.

[9] F. Wang, Y. Dong, J. Song, and J. Gu, "On the Performance of PassiveWorms over Unstructured P2P Networks," Proc. Int'l Conf. IntelligentNetworks and Intelligent Systems (ICINIS), pp. 164-167, Nov. 2009.

[10] R. Thommes and M. Coates, "Epidemiological Models of Peer-to-PeerViruses and Pollution," Proc. IEEE INFOCOM '06, Apr. 2006.