IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 2, 2015, Page.802-807, ISSN: 2347–8586

# Spatial-Temporal email Malware Propagation by using OLSR Protocol

**[1]M.Vijayapriya, [2]N.Anandh**
[1]PG Scholar, [2]Assistant Professor
Department of CSE, Anna University
Muthayammal Engineering College, Namakkal, India
[1]vijics43@gmail.com, [2]anandme1983@gmail.com

**Abstract-**Email is a basic service for computer users. The technique of email-borne malware will be highly effective. Email malware focuses on modeling the propagation dynamics which is a fundamental technique for developing countermeasures to reduce email malware's spreading speed and prevalence. Modern email malware exhibits two new features, reinjection and self-start. Reinjection is an infected user sends out malware copies whenever this user visits the malicious hyperlinks or attachments. Self-start refers to the behavior that malware starts to spread whenever compromised computers restart or certain files are visited. For address this problem, to derive a novel difference equation based analytical model by introducing a new concept of virtual dirty user. Propose a new analytical model to enhanced OLSR protocol which is a trust based technique to secure the OLSR nodes against the attack. The proposed solution called EOLSR is an enhancement of the basic OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network. All the nodes are authenticated and can participate in communication. In our protocol is able to achieve routing security and increase the packet delivery ratio and reduction in packet loss rate.

***Keywords:*** *Network security, email malware, propagation modeling*

## 1. INTRODUCTION

Malware short for malicious software is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software. With the escalating growth of communication and information systems, a new term and acronym invaded the digital world called as malware. It is a general term, which stands for malicious software and has many shapes (codes, scripts, active content and others). It has been designed to achieve some targets such as, collecting sensitive data, accessing private computer systems, even sometimes harming the systems. The malware can reach the systems in different ways and through multiple media; the most common way is the downloading process from the internet, once the malware finds its way to the systems, based on the functions of the malware the drama will begin.

## 2. RELATED WORK

In [1] C.C. Zou, D. Towsley, and W. Gong et al presents for there an electronic mail worm imitation replica that the books for the behaviors of correspondence users, counting email examination time and the likelihood of aperture and communication superfluous. Our annotations of news item lists recommend that an Internet send arrangement follows a heavy-tailed allocation in stipulations of swelling degrees, and facsimile it as an influence law friendship. To modify the topological collision, we evaluate message larva broadcast on power law topology with maggot dissemination on two other topologies: small planet topology and accidental grid topology.

In [2] S. Wen, W. Zhou, Y. Wang, W. Zhou et al presents A familiar examination for the preferable positions o awkward worm dissemination is at the greatly coupled nodes. To appraise the cause on uncomfortable maggot broadcasting by quarantining firm nodes, we recommend an illustration to symbolize the scattering practice of topological worms. Firstly, a communicable swelling can proliferate worms, and a susceptible user can be contaminated and turn into a novel communicable bump. In [3] Y. Wang, S. Wen, S. Cesare et al presents Research on larva broadcast has been conducted for more than a decade. However, customary models misjudge the scale of the tainted net that leads to proliferation errors because of partial and mistaken psychotherapy of the circulation course of action between each pair of nodes in the complex. For focus on analyzing the shape of broadcast errors and examined the collision of eliminating errors on the proliferation practice on two unusual types of worms. We encompass revealed by simulations that errors augment as added dissemination cycles are bent and quantified the errors under special transmission scenarios. In [4] S.M. Cheng, W.C. Ao, P.Y. Chen et al presents An amalgam malware on elegant phones can be propagated by both end-to-end messaging military via delicate social transportation and short-range wireless communiqué navy via spatial social interactions. stimulated from epidemiology, propose a novel differential equation-based model to analyze the mixed behaviors of delocalized infection and ripple based propagation for the hybrid malware in generalized social networks consisting of personal and spatial social relations. In [5] R. Thommes and M. Coates et al presents the fame of peer-to-peer (P2P) networks makes them an gorgeous objective to the creators of viruses and extra malevolent regulations. Freshly an amount of viruses premeditated explicitly to widen via P2P networks boast emerged. Toxic waste has also turned into ever more widespread as patent holders inject multiple decoy versions in order to hinder entry allotment. In this manuscript gain deterministic epidemiological models for the transmission of a P2P germ during a P2P network and the spreading of effluence.

**3.P2P MODEL NETWORK**

The recommend geometric models, which have capture the truthful topological in sequence. The sequential dynamics and the spatial dependence dilemma in the propagation modeling. nevertheless, all these model cannot present the reinfection and self-start process of up to date email malware. Their moving parts study the final stable state of epidemic spread based on SIS models, whereas we study the transient propagation dynamics of modern email malware. Second, there are some works which characterize the propagation dynamics of isomorphic malware, such as P2P malware, mobile malware and malware on online social networks.

The differential equations to present the propagation of P2P malware through a P2P network. The models are proposed for the mobile environment by presuming nodes meet each other with a probability. These works assume all individual devices are homogeneously mixed, and thus, they are unlikely to work in the real mobile environment. The models present the propagation of online social malware by simulations. Since these models are based on non-reinfection, they cannot be adopted to present the propagation of modern email malware.

**4. EXISTING SYSTEM**

These observations become the motivation of work to develop a new analytical model that can precisely present the propagation dynamics of the modern email malware. The spreading procedure can be characterized by a Susceptible-Infected-Immunized (SII), Susceptible-Infected-Resistant (SIR),Susceptible-Infected-Susceptible (SIS) process.

The major contributions of this paper are listed below:

To introduce a new concept of virtual nodes to address the underestimation in previous work, which can represent the situation of a user sending out one more round of malware copies each time this user gets infected. Perform empirical and theoretical study to investigate why and how the proposed SII model is superior to existing models. Modern email malware exhibits two new features, reinfection and self-start. For address this problem, to derive a novel difference equation based analytical model by introducing a new concept of virtual infected user.

In order to exclude the impact of other factors, we derive the SIS and SIR models on the basis of the SII model. First, a susceptible user can be immunized in SII model, but not in SIR model. Thus, we can revise equation (8) to obtain an SIR model as in

$P(X_i(t)=Imm.)=P(X_i(t-1)=Imm.)+r(t).$

$P(X_i(t-1)\text{-}Inf.).$

Second, an SIS model does not have the immunized state.We can have it by setting $P(X_i(t)=Imm.)=0$

$P(X_i(t)=Sus.)=(1-v(t)).P(X_i(t-1)=Sus.)$

$+r(t).P(X_i(t-1)=Inf.).$

A new analytical model to capture the interactions among the infected email users by a set of difference equations, which is together describe the overall propagation of the modern email malware. The proposed a novel SII model for the propagation of modern email malware.

This model is able to address two critical processes unsolved in previous models: the reinfection and the self-start. By introducing a group of difference equations and virtual nodes, it presented the repetitious spreading processes caused by the reinfection and the self-start.

### 4.1 LIMITATIONS

- It is malicious software
- Does not achieve greater accuracy
- It is not efficient
- Malware called topological scanning malware that spread based on topology information
- Packet delivery ratio is slow

## 5. VIRTUAL NODES

E-mail malware, recall that a compromised user may send out malware email copies to neighbours every time the user visits those malware hyperlinks or attachments. Malware emails are also sent out when certain events like computer restart are triggered. Thus, at an arbitrary time t, a user may receive multiple malware email copies from an identical neighbouring user who has been compromised. In order to represent the repetitious spreading process of their infection and the self-start, we introduce virtual nodes to present the kth infection caused by infected users opening the kth malware email copy.

## 6. PROPOSED SYSTEM

Analyzing the attack, propose a mechanism called enhanced OLSR (EOLSR) protocol which is a trust based technique to secure the OLSR nodes against the attack. The proposed solution called EOLSR is an enhancement of the basic OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network. In proposed system assumes that all the nodes are authenticated and can participate in communication i.e., all nodes are authorized nodes.

In our protocol is able to achieve routing security with increase in packet delivery ratio and reduction in packet loss rate. The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad hoc networks, which can also be used on other wireless ad hoc networks. OLSR is a proactive link-state routing protocol, which uses hello and Topology Control (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network.

Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. Link-state routing protocols such as Open Shortest Path First (OSPF) and IS-IS select a designated router on every link to perform flooding of topology information. IS-IS is an interior gateway protocol. It is a routing protocol designed to move information efficiently within a computer network. OSPF is a routing protocol for networks. It uses link state routing algorithm and falls into the group of interior routing protocols. It gathers link state information from available routers

In wireless ad hoc networks, there is different notion of a link, packets can and do go out the same interface; hence, a different approach is needed in order to optimize the flooding process. Using Hello messages the OLSR protocol at each node discovers 2-hop neighbor information and performs a distributed election of a set of multipoint relays (MPRs). Nodes select MPRs such that there exist a path to each of its 2-hop neighbors via a node selected as an MPR. These MPR nodes then source and forward TC messages that contain the MPR selectors.

This functioning of MPRs makes OLSR unique from other link state routing protocols in a few different ways: The forwarding path for TC messages is not shared among all nodes but varies depending on the source, only a subset of nodes source link state information, not all links of a node are advertised but only those that represent MPR selections.

Since link-state routing requires the topology database to be synchronized across the network, OSPF and IS-IS perform topology flooding using a reliable algorithm. Such an algorithm is very difficult to design for ad hoc wireless networks, so OLSR doesn't bother with reliability; it simply floods topology data often enough to make sure that the database does not remain unsynchronized for extended periods of time.

**5.1 Network Formation**

It consist of a set of nodes .Each and every node should have some kinds of ID, which is like N1, N2,…and Nn. Each node communicate with another node and all the nodes are authenticated.

**5.2 Data Transfer Through the Virtual Node**

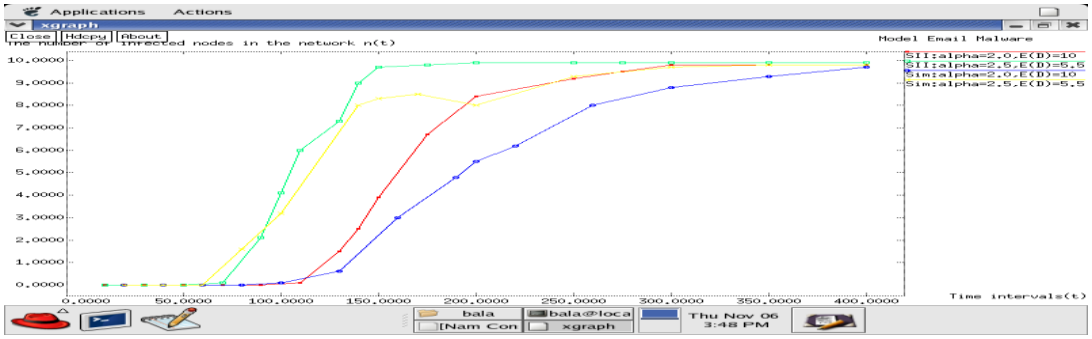
Virtual node can represent the situation of a user sending out one more round of malware copies each time this user gets infected. In order to represent the repetitious spreading process of the reinfection and the self-start, introduce virtual nodes to present the infection caused by infected users opening the malware email copy.

**5.3 Detection of Attackers**

To analyze the vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR) against a specific type of denial-of-service (DOS) attack called node isolation attack

Analyzing the attack, propose a mechanism called enhanced OLSR (EOLSR) protocol which is a trust based technique to secure the OLSR nodes against the attack. The technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks.

## PERFORMANCE EVALUATION




## 6. CONCLUSION

Susceptible-Infected-Susceptible (SII) model for the propagation of modern email malware and is used to address two critical processes unsolved in previous models: the reinfection and the self-start. The experiments showed that the result of Optimal Link State Routing Protocol (OLSR) model is close to the simulations. Propose a new analytical model to enhanced OLSR protocol which is a trust based technique to secure the OLSR nodes against the attack. The proposed solution called EOLSR is an enhancement of the basic OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network.

## REFERENCES

[1] C.C. Zou, D. Towsley, and W. Gong, “Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms,” IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105-118, Apr.-June 2007.

[2] S. Wen, W. Zhou, Y. Wang, W. Zhou, and Y. Xiang, “Locating Defense Positions for Thwarting the Propagation of Topological Worms,” IEEE Comm. Letters, vol. 16, no. 4, pp. 560-563, Apr. 2012.

[3] Y. Wang, S. Wen, S. Cesare, W. Zhou, and Y. Xiang, “Eliminating Errors in Worm Propagation Models,” IEEE Comm. Letters, vol. 15, no. 9, pp. 1022-1024, Sept. 2011.

[4] S.M. Cheng, W.C. Ao, P.Y. Chen, and K.C. Chen, “On Modeling Malware Propagation in Generalized Social Networks,” IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.

[5] R. Thommes and M. Coates,“Epidemiological Modelling of PeertoPeer Viruses and Pollution,” Proc. IEEE INFOCOM ’06, pp. 1-12, 2006.

[6] M. Fossi and J. Blackbird, “Symantec Internet Security Threat Report 2010,” technical report Symantec Corporation, Mar. 2011.

[7] P. Wood and G. Egan, “Symantec Internet Security Threat Report 2011,” technical report, Symantec Corporation, Apr. 2012.

[8] Z. Chen and C. Ji, “Spatial-Temporal Modeling of Malware Propagation in Networks,” IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1291-1303, Sept. 2005.

[9] C. Gao, J. Liu, and N. Zhong, "Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis," Knowledge and Information Systems, vol. 27, pp. 253-279, 2011.

[10] J. Xiong, "Act: Attachment Chain Tracing Scheme for Email Virus Detection and Control," Proc. ACM Workshop Rapid Malcode (WORM '04), pp. 11-22, 2004.

[11] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling Propagation Dynamics of Social Network Worms," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 8, pp. 1633-1643, Aug. 2013.

[12] (1999) Cert, advisory ca-1999-04, Melissa Macro Virus, http:// www.cert.org/advisories/CA-1999-04.html, 2009.

[13] Cert, Advisory ca-2000-04, Love Letter Worm, http://www.cert.org/advisories/CA-2000-04.html, 2000.

[14] M. Calzarossa and E. Gelenbe, Performance Tools and Applications to Networked Systems: Revised Tutorial Lectures. Springer-Verlag, 2004.

[15] G. Serazzi and S. Zanero, "Computer Virus Propagation Models," Proc. 11th IEEE/ACM Int'l Conf. Modeling, Analysis and Simulations of Computer and Telecomm. Systems (MASCOTS '03), pp. 1-10, Oct. 2003.