ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

On Modeling Malware Propagation in E-Mail by Using OLSR Protocol

M.Vijayapriya[1], N.Anandh[2]

PG Student [CSE], Dept. of CSE, Muthayammal Engineering College, Rasipuram, Tamil Nadu, India[1]

Assistant Professor, Dept. of CSE, Muthayammal Engineering College, Rasipuram, Tamil Nadu, India[2]

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

I. 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. 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

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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.

II. 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-Sesceptible(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. 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.

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

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 the reinfection and the self-start.

III. 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

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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.

Multipoint Relay (Mpr)
Multipoint relays (MPR) are nodes in Wireless ad hoc network that do the job of relaying messages between nodes. They also have the main role in routing and selecting the proper route from any source to any desired destination node. MPRs advertise link-state information for their MPR selectors (a node selected as a MPR) periodically in their control messages. MPRs are also used to form a route from a given node to any destination in route calculation. Each node periodically broadcasts a Hello message for the link sensing, neighbor detection and MPR selection processes. Each node can get topology up to 2 hops from Hello messages. The information about the symmetric one hop and two hop neighbors is used to calculate the MPR set. Each node selects set of neighbor nodes as MPRs from among 1-hop neighbors with symmetric link, which covers all the 2-hop neighbors and records in MPR selector table.MPR is recalculated when a change in 1-hop or 2-hops neighborhood topology is detected. Every node periodically broadcasts list of its MPR selectors instead of the whole list of neighbors. Upon receipt of MPR information, each node recalculates and updates routes to each known destination. In order to exchange the topological information, the topology control (TC) message is broadcast throughout the network. Only MPRs need to forward TC messages.

Intermediate System to Intermediate System (IS-IS)
IS-IS is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. It accomplishes this by determining the best route for datagram's through a packet-switched network. IS-IS (pronounced "i-s i-s") is an interior gateway protocol, designed for use within an administrative domain or network. This is in contrast to Exterior Gateway protocols, primarily Border Gateway Protocol (BGP). IS-IS is a link-state routing protocol, operating by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. Like the OSPF protocol, IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets (datagrams) are then forwarded, based on the computed ideal path, through the network to the destination

OSPF
A link-state routing protocol is one of the two main classes of routing protocols used in packet switching networks for computer communications (the other is the distance-vector routing protocol). Examples of link-state routing protocols include open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS). The link-state protocol is performed by every switching node in the network (i.e., nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. The collection of best paths will then form the node's routing table. This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors. In a link-state protocol the only information passed between nodes is connectivity related. Link-state algorithms are sometimes characterized informally as each router 'telling the world about its neighbors"

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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.

Attacker Performance

Malware to disrupt computer operation, gather sensitive information, or gain access to private computer systems. For modern email malware, recall that a compromised user may send out malware email copies to neighbors every time the user visits those malware hyperlinks or attachments.

SYSTEM ARCHITECTURE:

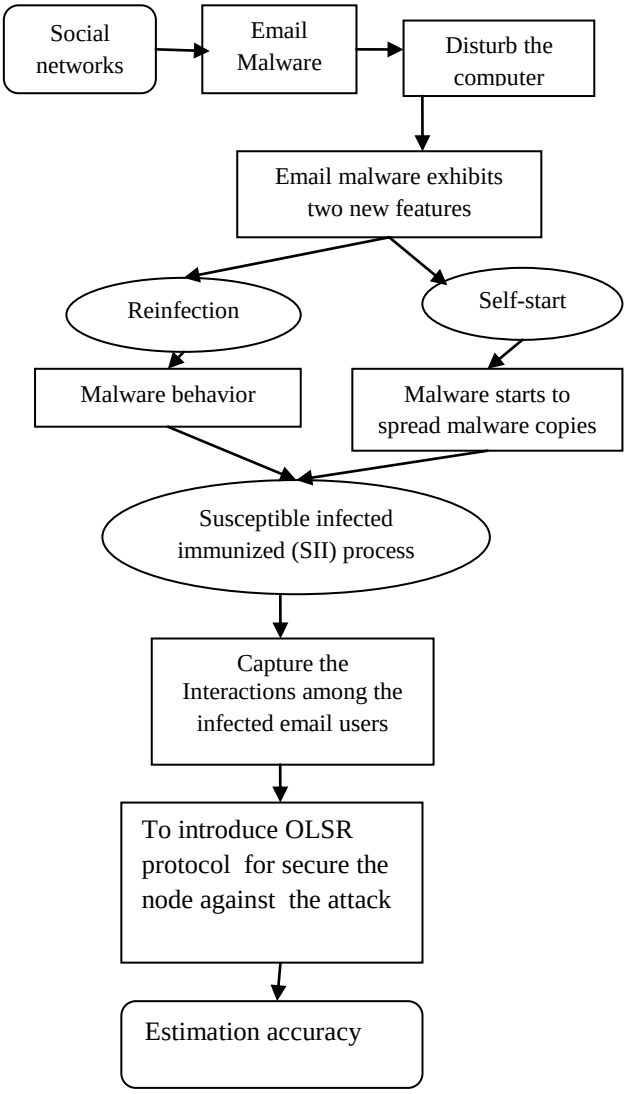

Fig : system architecture

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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.

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.

IV. EXPERIMENTAL RESULTS

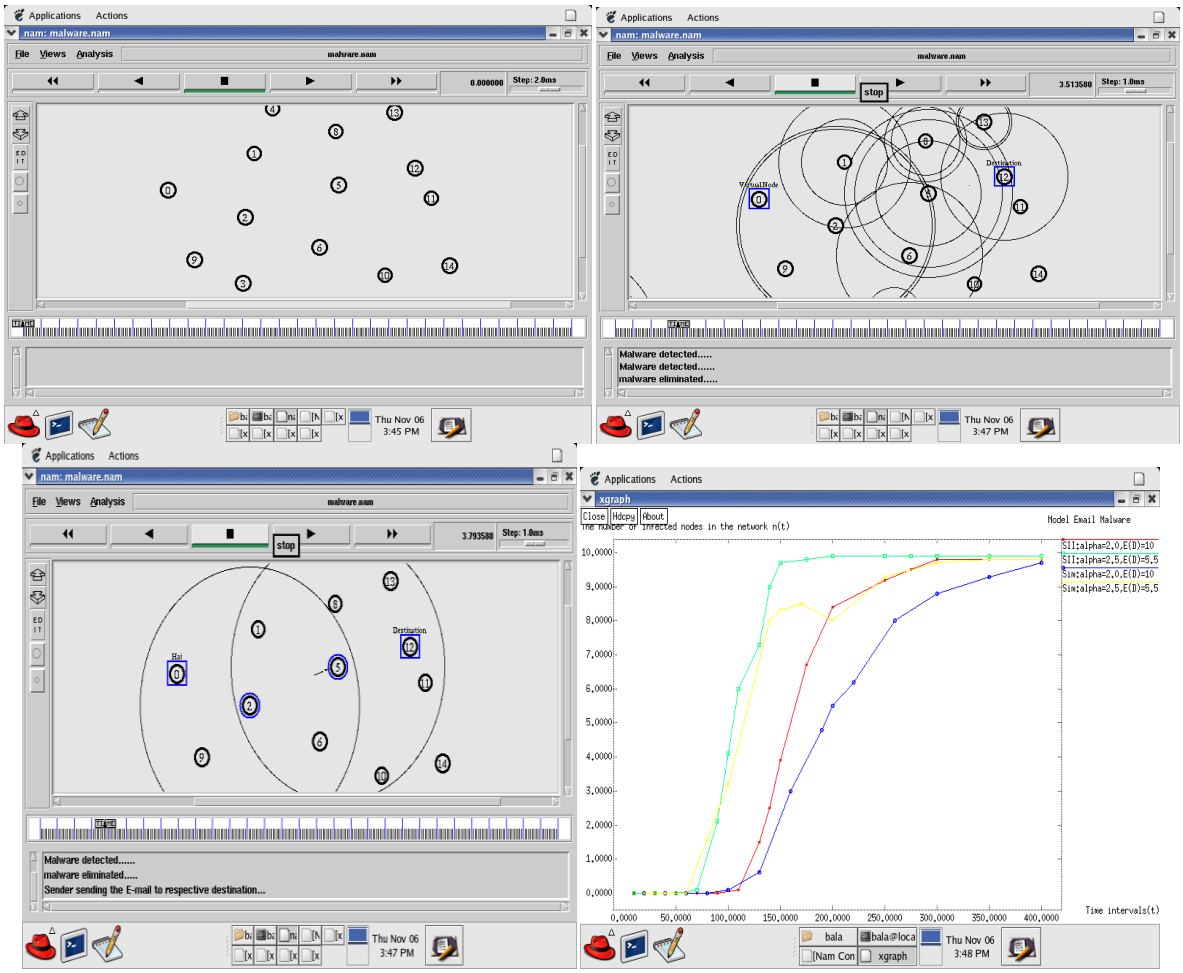

Fig.(1) Network formation. (2) Data transfer through the virtual node. (3) To identify the malware node and elimate for those node. (4) Performance evaluation

V. 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

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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] M. Calzarossa and E. Gelenbe, Performance Tools and Applications to Networked Systems: Revised Tutorial Lectures. Springer-Verlag, 2004.
[14] 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.
[15] B. Rozenberg, E. Gudes, and Y. Elovici, "SISR: A New Model for Epidemic Spreading of Electronic Threats," Proc. 12th Int'l Conf. Information Security, pp. 242-249, 2009.