Containment of Worms in packet Dispersion Technique

Rohitkumar Rudrappa Wagdarikar
Computer Science and Engineering,
Symbiosis Institute of Technology and Science,
Jawaharlal Nehru Technological University, Hyderabad, India.
E-mail- rohit.wagdarikar@yahoo.com

Manik A. Raichurakar
Computer Science and Engineering,
Bandari Srinivas Institute of Technology, Chevella,
Jawaharlal Nehru Technological University, Hyderabad,India.
Email- manikraichurakar@gmail.com

Abstract: - Self-propagating codes, called worms. Network worms have the potential to infect many vulnerable hosts on the network before human countermeasures take place. In real growing world, Network Security is very necessary. To provide a secure, reliable network system, we are going to develop such an application which provides a high security in network. The dispersion technique is very useful to provide high security in Network. Packet Dispersion provides facility to hide data from hacker and this is possible by dispersion of packet. In dispersion technique at the source end packet are divided into to the chunks and these chunks are then distributed over the network. While distributing these chunks of the packets there will be possibilities of worms those infects these chunks of packets The aggressive scanning traffic generated by the infected hosts has caused network congestion, equipment failure, and blocking of physical facilities. Once these chunks will get infected then there is a possibility, is that the whole system will get shutdown. So in this technique specifically, for scanning of worms, we are able to provide a precise condition that determines whether the worm spread will eventually stop and to obtain the distribution of the total number of hosts that the worm infects. We then extend our results to contain preference scanning worms.

Index Terms— packet dispersion, Inclination branching process model, Preference scanning worms, worm containment, Data Security using Packet dispersion, Internet scanning worms, Active Worms.

IJSER

1 INTRODUCTION

The Internet has become critically important to the financial viability of the national and the global economy. Meanwhile, we are witnessing an upsurge in the incidents of malicious code in the form of computer viruses and worms. One class of such malicious code, known as random scanning worms, spreads itself without human intervention by using a scanning strategy to find vulnerable hosts to infect.

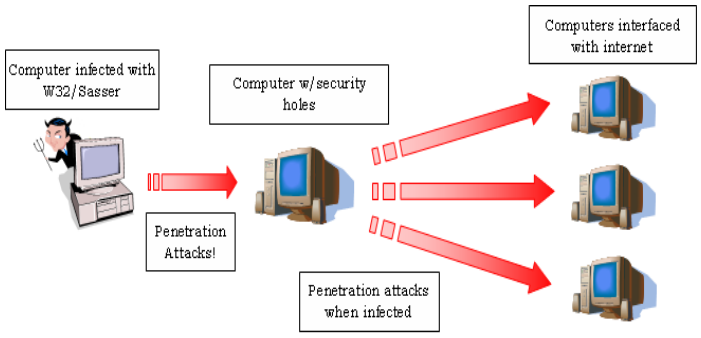

Figure 1The spread of Worm

As shown in figure 1. The worm is send by a user to a victim. Later on that worm is spreading over the network. The goal of our research is to provide a model for the inclination branching process model for characterizing the propagation of Internet worms. Basically user knows the name and the definition of worms, but sometimes due to the validity or the lack of latest updates of the worm containment system, system cannot find the worms. Then these worms are start spreading into the network. The model is developed for preference scanning worms and then extended to inclination scanning worms. This model leads to the development of an inclination worm containment strategy that prevents the spread of a worm beyond its early stage. Specifically, for preference scanning worms, we are able to provide a precise condition that determines whether the worm spread will eventually stop and obtain the distribution of the total number of hosts that the worm infects. We then extend our results to contain inclination scanning worms. Propagation of random scanning worms and the corresponding development of inclination containment mechanisms is that prevent the spread of worms beyond their early stages. This containment scheme is then extended to protect an enterprise network from a preference scanning worm. A host infected with random scanning worms finds and infects other vulnerable hosts by scanning a list of randomly generated IP addresses. Worms using other strategies to find vulnerable hosts to infect are not within the scope of this work. The aggressive scanning traffic generated by the infected hosts has caused network congestion, equipment failure, and blocking

of physical facilities such as subway stations, 911 call centers, etc. consider code red worm version 2that exploit buffer overflow vulnerability in Microsoft IISWebserver, over the period of less than 14 hours it infected 359,000 machines it cost near about $1.2billion.

Packet dispersion in IP networks is a mechanism in which application packets are dispersed between parallel paths leading from the source to the destination, based on a predefined dispersion strategy. Packet dispersion can be implemented by the source application or by nodes in the network. There are two types of Packet Dispersion techniques: Packet Pair Dispersion, Packet Train Dispersion. In a Packet Pair Dispersion, Two equal sized packets are sent back to back through the network. In a Traffic Train Dispersion, multiple back to back probe packets are sent through the network.
Packet dispersion can be implemented through a variety of strategies, which of these are following:

I. Deterministic scheduling dispersion

a. Periodic dispersion – session packets are dispersed in a periodic schedule manner over the routes repeatedly. For example, if the schedule is (i, i, i, j, j) then in every cycle 3 packets in a row are sent over path pi, and then the following two packets are sent over path pj, where this schedule repeats cyclically.

b. Deterministic round robin dispersion – a special case of periodic dispersion where packets are sent in a round robin fashion (cyclic schedule) over the paths.

II. Random packet dispersion – for each packet of the session, the dispersing device picks randomly one of the paths leading to the destination and sends the packet over it. The traditional delivery of packets over a single path is referred to as a no-dispersion strategy. We will assume that the packet dispersion strategies are executed in session context [10].

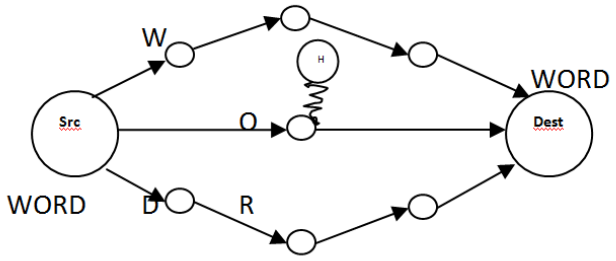

Figure 2. WORD Transmission on MANET using Packet Dispersion

There is a possibility that when a sender chooses an intermediate link to send some message to destination, the intermediate link may give problems such as the intermediate node may not forward the packets to destination, it may take very long time to send packets or it may modify the contents of the packet. In network as there is no retransmission of packets once it is sent, hence care is to be taken that packets are not lost. Note that a misbehaving node can either be the sender or the receiver of the next-hop link. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet. It will not be forwarded further. The nodes which do not forward the packets to neighboring nodes called as selfish nodes.

The node level modules are following:

Module 1: Sender module (Source Node) The task of this module is to read the message and then divide the message into packets, send these packets to receiver through the intermediate node and receive acknowledgement from the receiver node through the intermediate node.

Module 2: Intermediate module (Intermediate Node) The task of this module is to receive packet from sender and send it to intermediate node toward the destination.

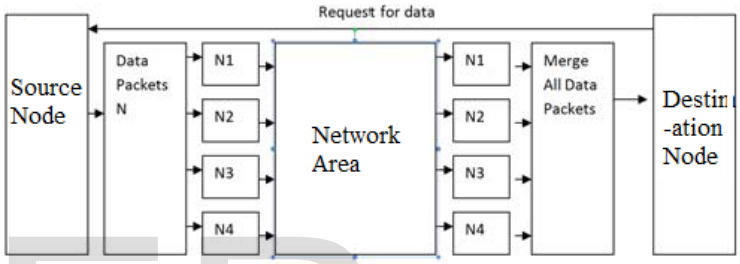

Figure 3 Architecture of Packet Dispersion

Module 3: Receiver module (Destination Node). The task of this module is to receive message from the intermediate node, take out destination name and hash code and decode it. Compare the hash code of source node and destination node for security purpose.

2. RELATED WORK

The following list of papers shows the relative work carried out for Containment of worms in packet dispersion technique and possible solutions given.

1. Securing a Network by Modeling and Containment of Worms Using Preference Scanning. by R.R.Wagdarikar, R.C.Maheshwar,M.A. Raichurakar - IJRCCT Vol 2, No 10 (2013).

2. Data Security Using Packet Dispersion in MANET. By R.R.Wagdarikar, R.C.Maheshwar, A.G.Deshmukh- IJIET Vol. 2 Issue 3 June 2013

3. S. Sellke, N. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," Proc. IEEE Int'l Conf. Dependable Systems and Networks, pp. 528-537, 2005.[1] This paper focuses on Modeling and Automated containment of Worms at early phase.

4. H.Andersson and T. Britton, "Stochastic Epidemic Models and Their Statistical Analysis," Lecture Notes in Statistics, vol. 151, 2000.[2] This paper focus on branching process model for characterizing the propagation of Internet worms.

5. Packet Dispersion in IEEE in 802.11 Wireless Networks: This paper focuses on packet dispersion in Wireless LAN (WLAN's) and types of dispersion.

6. N. Weaver, S. Staniford, and V. Paxson, "Very Fast Containment of Scanning Worms," Proc. Usenix Security Symp., pp. 29-44, 2004.Z Z [4]This Paper focusing on very fast Containment of Scanning Worms.

3. PROPOSED SYSTEM

The Packet Dispersion technique divides data into sub packets and disperses those packets in network. Dispersion means the sending different packets to different nodes. While sending these packets to the different nodes that particular system will check for that worm and performs the containment of worms and this node will inform to the next node for the detected worms.

Past Trends: Few years ago, encryption and decryption algorithm was used to provide security. Once a node is compromised, the hacker can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. And to provide the security against the worms, Random scanning of worms is performed. In this model system will generate random IP address for scanning, most of the time this system will generate dark IP address, and this system even start scanning on this dark IP addresses. It will take a long time to detect a worm in the Network. Scanning a worm in the dark IP address space is total west of time. Scanning performing in the dark IP address space worm will get infect the other system present the Network.

Current trends: Now days, organizations became large so they must require good application which manages the security of whole organization. Inclination branching process model gives flexible facilities to the network with better performance. We provide the facilities that needed for the organization.

Future Trends: This model provides the facility that makes a flexible and reliable network system. We have to provide some future trends such give a powerful network system that contains a worm in inclination basis. Those give strong algorithm for worm containment technique.

Goals: The goal of "Containment of worms in packet dispersion technique" is to secure the network get infected by worms in early phase by providing an inclination branching process model. As shown in figure 4, when sub packet will received at INT_Node2 (Intermediate node 2) then it will start the containment of worm. When worm will get contained then that INT_NODE 2 will spread the definition of contained worm.

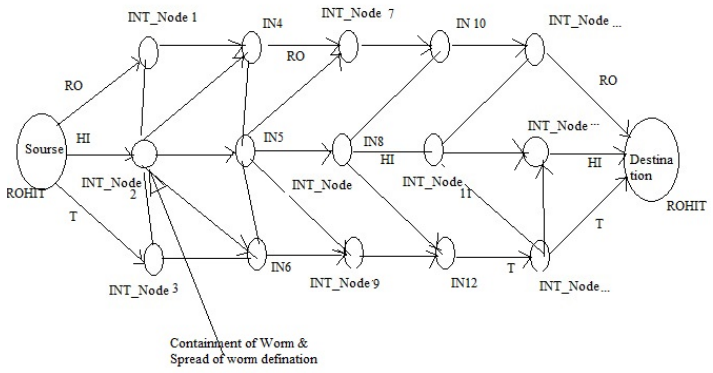

Figure4 Containment of worms.

Problem Definition: The dispersion technique is very useful to provide high security in Network. Packet Dispersion provides facility to hide data from hacker and this is possible by dispersion of packet. In dispersion technique at the source end packet are divided into to the chunks and these chunks are then distributed over the network. While distributing these chunks of the packets there will be possibilities of worms those infects these chunks of packets .The aggressive scanning traffic generated by the infected hosts has caused network congestion, equipment failure, and blocking of physical facilities. Once these chunks will get infected then there is a possibility, is that the whole system will get shutdown.

4. SYSTEM MODEL

The modules are as follows: Data Module, Dispersion Module, Routing Module, Inclination Module and Containment Module.

Data Module: This module Sink Node will request to the sensor node for data and its details. Then Sensor node will receive acknowledgment from the Sink node with its details. Sensor node gather appropriate data required by the Sink node and get details about time to live and chunks.

Dispersion Module: In this module sensor divides data into sub packets and disperses those packets in the network. Dispersion means sent different packets to different nodes.

Routing Module: This module is used to route the packet in the network. This module decides that which packet to be sends to which node and in this module it will find trusted and selfish nodes and make a group of trusted node and send the packets to the intermediate trusted nodes.

Inclination Module: Once the packet reached to the intermediate trusted node then it will start inclination branching process module. In an Inclination branching process module, user selects a worm that is identified by currently running worm containment system and perform containment of worm and then informs to the next node.

Containment Module: In this module it starts searching for user selected worm that is specified in Inclination branching process module. While searching, it will search in all file and

folders of the system through advance search system.
In existing system, source Node will request to the destination node for data and its details. Then destination node will receive acknowledgment from the source node with its details. Destination node gather appropriate data required by the source node and get details about time to live and chunks. Then destination divides data into sub packets and disperses those packets in the network. Once the sub packets reached at the destination it will simply forward this sub packet to the next node in the network without checking the threat of worms or some node will perform the check for the worms, but they will not inform to the next node in the network for the currently contained worm. And the aggressive scanning traffic generated by the infected hosts has caused network congestion, equipment failure, and blocking of physical facilities. Once these chunks will get infected then there is a possibility, is that the whole system will get shutdown.

5. ALGORITHM FOR CONTAINMENT OF WORMS IN PACKET DISPERSION TECHNIQUE

We have used the triplet of SENSOR_NODE -> INT_NODE -> SINK_NODE as an example to illustrate Packet Dispersion. Where SENSOR_NODE is assumed as the source node, INT_NODE is the intermediate node and SINK_NODE is the destination node.
Nomenclature:
Pkt_Count = the number of the message packets sent,
Pkt_Miss = the number of the 2ACK packets missed,
d = the acknowledgement ratio,
WT = waiting time, i.e., the maximum time allotted to receive 2ACK packet.

5.1 Data Module:

Sink Node: Request for Data to the sensor node.
Sensor Node: Accept the request from sink node. Extract the Sink Node details.
Gather the details of data, size of data, the time to live and details of chunk.

5.2 Dispersion Module:

At node SENSOR_NODE
While (true) do
Read the destination address;
Read the message;
Find the length of the message.
Pkt_Miss=0, Pkt_Count=0, WT=20 ms, d=0.2,
2ACK Time=Current Time (Acknowledgement accepted time) – Start Time.
While (length > 64 bytes) do
Take out 64 message packet;
Length = length – 64;
Encode message using hash function;
Send message along with the hash key;
Pkt_Count++ ;

Receive 2ACK packet;
If (2ACK time > WT) then
Pkt_Miss++;
End
End
If (length < 64 bytes) then
Encode message using hash function;
Send message along with the hash key;
Pkt_Count++;
Receive 2ACK packet;
If (2ACK time > WT) then
Pkt_Miss++;
End
End
End

At node SINK_NODE:
While (true) do
Read message from INT_NODE;
Take out destination name and hash code;
Decode the message;
Rearranges all messages;
If (Pkt_Count==total_chunk)
Successfully received the messages;
Else
Retransmission of messages;
End
Send 2ACK packet to INT_NODE;
End

5.3 Routing Module:

In this module it will start searching for trusted nodes and start searching for the worm.
At node INT_NODE
Find out Trusted nodes and Selfish nodes.
While (true) do
Send the request to all intermediate nodes.
If (Ack==true) then
Add it to trusted group nodes
Else
Declare it as a selfish node.
End if
End

While (true) do
Read message from source SENSOR_NODE
Start Containment Module for the entire Host.
In INT_NODE if (worm file=true)
{ Worm Found SENSOR_NODE}
Send the worm definition to the next INT_NODE.
INT_NODE will start the containment of worm and stop spreading of worms in the next INT_NODE.
End

6. RESULT AND FUTURE SCOPE

In this system we will perform the worm containment strategy on the Intermediate nodes of network system which leads to the development of an inclination worm containment strategy that prevents the spread of a worm beyond its early

stage. Further the scheme can also be extended to obtain the probability that the total number of hosts that the worm infects is below a certain level, as a function of the scan limit. The insights gained from analyzing this model also allow us to develop an effective and automatic worm containment strategy that does not let the worm propagate beyond the early stages of infection.

7. CONCLUSION

In this paper, we have studied the problem of combating Internet worms. To that end, we have developed a Inclination branching process model to characterize the propagation of Internet worms. And the dispersion technique is very useful to provide high security in Network. Packet Dispersion provides facility to hide data from hacker and this is possible by dispersion of packet. In dispersion technique at the source end packet are divided into to the chunks and these chunks are then distributed over the network. While distributing these chunks of the packets there will be possibilities of worms those infects these chunks of packets .The aggressive scanning traffic generated by the infected hosts has caused network congestion, equipment failure, and blocking of physical facilities. Once these chunks will get infected then there is a possibility, is that the whole system will get shutdown. So in our system we will perform the branching process model and perform the containment of worms. With the help of the will perform the early phase of worm detection by sending the contained worm definition to the next intermediate node in the network. And these intermediate nodes will stop the spreading of worms.

IJSER

REFERENCES

[1] Securing a Network by Modeling and Containment of Worms Using Preference Scanning. by R.R.Wagdarikar, R.C.Maheshwar,M.A. Raichurakar -IJRCCT Vol 2, No 10 (2013)

[2] Data Security Using Packet Dispersion in MANET. by R.C.Maheshwar, R.R.Wagdarikar, A.G.Deshmukh-IJIET Vol. 2 Issue 3 June 2013

[3] S. Sellke, N. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," Proc. IEEE Int'l Conf. Dependable Systems and Networks, pp. 528-537, 2005.

[4] "The Cost of Code Red: $1.2 Billion," USA Today News, http:// www.usatoday.com/tech/news/2001-08-01-code-red-costs.htm, 2001.

[5] N. Weaver, S. Staniford, and V. Paxson, "Very Fast Containment of Scanning Worms," Proc. Usenix Security Symp., pp. 29-44, 2004.Z Z

[6] Z. Chen, L. Gao, and K. Kwiat, "Modeling the Spread of Active Worms," Proc. IEEE INFOCOM '03, pp. 1890-1900, 2003.

[7] C.C. Zou, W. Gong, and D. Towsley, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," Proc. ACM Workshop Rapid Malcode, pp. 51-60, 2003.

[8] D.J. Daley and J. Gani, Epidemic Modelling, An Introduction. Cambridge Univ. Press, 1999.Computer Economics, "Economic Impact of Malicious Code Attacks," http://www.computereconomics.com/cei/press/ pr92101.html, 2001.

[9] Mingzhe Li, Mark Claypool and Bob Kinicki , Packet Dispersion in IEEE in 802.11 Wireless Networks , P2MNet Tampa, Florida, November 14, 2006

[10] Panagiotis Papadimitratos *, Zygmunt J. Haas, Secure Data Transmission Model in MANET, Ad Hoc Networks 1 (2003) 193–209.