IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Virus Spreading Control over network by using Black and White Algorithm

Dr. B.Pavan Kumar[1] V Dhanushya[2] A Dileep[3] B Anusha[4] N Hithesh[5]

[1]Associate Professor, [2345]UG Student, Department of Computer Science and Engineering,
[12345]Siddharth Institute Of Engineering & Technology, Tirupathi, Andhra Pradesh, India,

ABSTRACT

Although difficult, controlling viral propagation over intricate networks on a tight budget has received a lot of attention. In order to restrict viral spread, this article seeks to answer the combinatorial, discrete resource allocation problems (RAPs). A co-evolutionary algorithm with network-community-based decomposition is offered as an evolutionary divide-and-conquer method to address the challenges of growing network scales and boost solving effectiveness. It is distinguished by its use of a community-based dividing strategy and cooperative co-evolutionary philosophy. Secondly, in order to decrease the time complexity, NCD-CEA separates a network into numerous communities using a modified community detection technique, resulting in a clustering of the variables that are most important to the solution. Then, the problem and the global swarm are divided into smaller problems and smaller swarms using low-dimensional Second, an alternate evolutionary strategy that promotes the evolution of sub swarms and the global swarm in turn, with sub solutions assessed by local fitness, is meant to produce high-quality solutions.

Index Words : *Resource distribution, networked systems, spreading control, cooperative coevolution (CC).*

INTRODUCTION

In the past, the spread of viruses, such as infectious illnesses and computer malware, has resulted in significant economic loss and public fear [1]. The effectiveness of necessary resource interventions in controlling viruses has been established. For instance, in underdeveloped nations, malaria in Africa has long been a serious threat to human life, but between 2000 and 2015, because to the widespread use of preventive measures, it has decreased by 40%. (insecticide-treated nets). Anti-malware software is essential to guaranteeing the security of networking equipment after the recent global cyber attack, known as the Wanna Cry ransomware attack, which affected more than 150 countries and resulted in billions of dollars in losses. While simulating the propagation of a virus in the real world is difficult due to high costs and a high chance of control failure, mathematical modelling and analogue control become useful tools for determining public policies in actual crises. Relevant studies in the prevention of virus spread can be categorised into three complimentary study areas. Topology Adjustment Early complex network theory investigations [3], [4] suggested that network topologies had a substantial impact on spreading dynamics. Hence, quite a few topological adaptation techniques were created, For instance, isolating the nodes at high risk of infection [7]-[10], eliminating some connections using topology-manipulative techniques [3], [5] removing a portion of nodes with high degree centrality [5], [6]. These methods might, to some extent, effectively stop the spread of viruses, but they frequently neglected the cost of adaptation [3, [6], [8], or severely damaged network connectivity [3, [5]–[7].

B. Intervention at Nodes The node intervention focused on changing the node state or lowering infection rates rather than breaking off contacts in networks, in contrast to topology adaptation.

LITERATURE SURVEY

Describe a network. "Any group of interlinking lines resembling a net, a network of roadways or an integrated system, a network of alliances" is the definition of "network." Simply described, a computer network is a collection of linked computers.

Network Types

P2P: A peer-to-peer network is one in which each computer serves as both a client and a server and lacks a dedicated server. When there are ten or fewer users nearby and they are close to one another, this is a viable networking option. The proper people could not have access to the right resources in a peer-to-peer network because users, not administrators, will be determining permissions for shared resources. This is only advised in circumstances when security is not a concern since, more critically, the incorrect persons might have access to the incorrect resources.

CLIENT/SERVER: This form of network uses a dedicated server or servers to service a large number of users. In order to access the server(s) and run programmes or download files, clients must log in. One or more administrators can control security and permissions, which prevents the aforementioned computer novices from tampering with things they shouldn't be. Also, this kind of network enables convenient backup services, lowers network traffic, and offers a wide range of other services that are included with the network operating system (NOS).

CENTRALIZED: This client/server model, which is most frequently used in UNIX environments, also uses "dumb terminals" as clients. The client might not have a floppy drive as a result of this. All applications and processing are done on the server(s), whether it be a hard drive or CDROM. As you can expect, this calls for incredibly expensive and quick server(s). On this type of network, security is extremely high, albeit a similar level of security can be attained by using an NT server with the proper settings.

The Reference Model for ISO/OSI

Seven different types of communications are categorised into layers by the Open Systems Interconnect (OSI) Reference Model developed by the International Standards Organization (ISO). To view Figure 1.1, All the way down to the actual network hardware, like the network interface card in a computer, and the wires that link the cards together, each layer depends on the services offered by the layer above it. The knowledge that they exist is useful. and that each layer depends on the functions of the one below it to function. The features of the OSI reference model, including the responsibilities of each layer, the devices utilised in each layer, and the accompanying protocols, are shown in Table 1.1 below.

Threats to the Network: Forms and Sources

Network threats come in a wide variety of forms. In fact, we can discuss the security features of networks. We'll discuss the several hazards that affect networked computers first, followed by some steps you may take to safeguard yourself from various dangers.

Denial-of-Service: The worst and most challenging to stop are arguably DoS (Denial-of-Service) attacks. These are the worst because they are the easiest to launch, the hardest to track (often even impossible), and that the functionality of each layer depends on that of the layer below it. Table 1.1 below lists the characteristics of the OSI reference model, including the roles played by each layer, the devices used in each layer, and the associated protocols.

Network Threats: Sources and Shapes

There are many different types of network dangers. In reality, we can talk about network security aspects. We'll talk about the numerous risks that networked computers face before outlining some preventative measures you can take.

Denial-of-Service: DoS (Denial-of-Service) attacks are undoubtedly the worst and hardest to defend against. They are the worst since they are the most straightforward to launch and the most challenging to track (often even impossible), However before granting command shell access, the host must be certain that the requester is a legitimate recipient, such as a local administrator.

Unlawful Command Execution: Having a stranger or someone you don't trust be able to access your server machines and issue instructions is plainly unpleasant. The severity of this issue can be divided into two categories: administrator access and typical user access. A regular user can access a system in ways that an attacker shouldn't be able to (reading files, sending them to other people, etc.). So, an attacker may only require this level of access. On the other side, a hacker might want to alter a device's setup.

User-Started Malware

Users rarely receive security awareness training. Even when they do receive this training, users frequently make errors that have a negative impact on the security environment of a company. Moreover, it is possible to deceive users into taking activities that violate security and entirely bypass perimeter protection systems. A wide range of user behaviours jeopardise security. Some of these activities are unintentionally carried out, meaning that the user is duped into carrying out an activity or is unaware of the risk involved. The standard illustration is when a person opens an infected email attachment. A user downloading a malicious programme from the Internet is another frequent occurrence. People who are unsure of how to run executable files that arrive as email attachments, or to download and run code from dubious websites will carry out additional steps that could jeopardise security. Another instance is when users download and install well-known, unauthorised software, which many administrators forbid. The security perimeter can be totally bypassed by malware as a result of people putting illicit wireless networking devices on their workstations more recently. Finally, some users act maliciously straight up. In this scenario, the user will knowingly deploy malware—created by them or possibly an accomplice—that will be used to infiltrate the company's software systems. These user-initiated security breaches have a substantial impact and are regrettably becoming more frequent. The malicious programme opens back doors, deploys root kits, uses keyboard loggers, steals or deletes important data, and carries out several other actions.

RECENT WORKS

The current system uses a variety of conventional defence techniques to deliver "Defense in Depth" network security, which aims to completely eradicate or drastically limit the harm caused by user-initiated malware. Typical techniques include antivirus software, hardware and software firewalls, intrusion detection and prevention systems, honeypots, and personal firewalls. The benefit of these techniques is that they may be used to regulate the ingress or egress traffic generated by the application and safeguard the system from virus infection.

LIMITATIONS

Yet, these protection strategies are insufficient to stop malware that is executed at the user's request. Prevention falls short. Treatment is using the recommended method.

The objective of this project is to provide network security. Eliminating user-initiated malware execution will increase security. Security and the implementation of a tactic known as "Defense in Depth" can also be achieved using several conventional protection techniques, such as anti-virus software and personal firewalls. Nevertheless, these techniques are only useful when they correctly identify signatures. The goal of this project is to provide "Defense in Depth" network security, which has the advantage of preventing or significantly reducing damage from User-Initiated Malware.

Potential System Benefits:

• Presenting a straightforward but efficient approach to enhancing network security based on preventing user-initiated malware execution.

• Outlining why common strategies fall short in this situation.

• Creating a test system that utilises the module

• A verification plan describing how this method can be implemented by modifying a default operating system loader to incorporate references to a database of cryptographic hashes of module executables.

Architecture Diagram

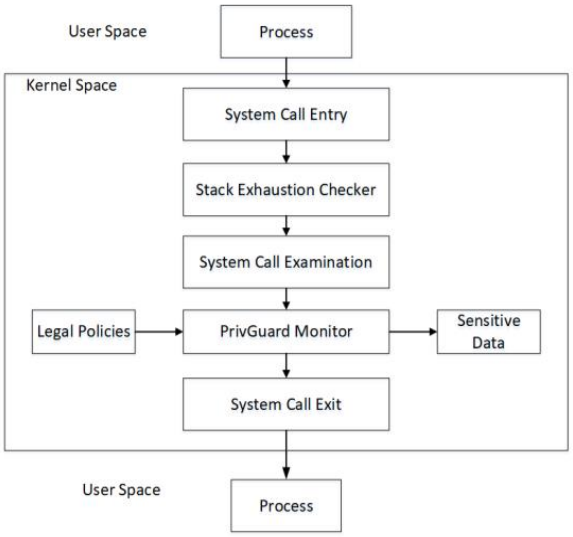

Fig 1: System Architecture

ALGORITHM:

1. *Administrator login in to the safe code Registry.*
2. *He checks the safe code Registry.*
3. *He gets all the system's Processes in the safe code Registry.*
4. *It generates a Hash Value for all the Processes in the registry.*
5. *The generated hash value will be stored in Registry.*
6. *Administrator approves some Processes to be executed by other people in the registry.*
7. *Administrator log off from the Registry.*
8. *user executes any processes in the system.*
9. *A hash value is generated for that process in the registry.*
10. *The generated hash value will be stored in the Registry.*
11. *The generated hash value will be compared with the previous hash code.*
12. *If the hash value is equal, then user can execute that process.*
13. *Otherwise process doesn't execute.*

WORKING MODULES

ADMINISTRATION MODULE: The system owner is given a user-friendly gui environment so he can manage his machine. The appropriate user credentials, such as a user login and password, are delivered to the administrator along with a secure login. The configuration or initialization of the LOCAL system state is the administrator's responsibility. The system administrator has the choice of classifying the system processors as legitimate, malicious, or unknown. The anti-malware verification Module for local workstations can be turned on or off by the administrator.

Module for Malware Verification: The "killer" module runs on the local machine as a TSR (Termnate Stay Resident) programme. It continuously reads process information from the local operating system's process stable to determine the list of active processors. The killer module locates the associated programme binary-file and generates the hash code for the complete file's contents for each process that is presently running or has just been started. The freshly produced hash code and the programme name are checked against the list of permitted processes. If a process is not on the list of allowed processes, it is first classified as unknown or malware before being stopped in its tracks. (The alleged murderer). The procedure may execute if it is on the list of approved processes.

Initialization/Setup Module: The administrator will utilise this module to authorise each pre-tested programme or process on the local workstation. The core content of the program's binary file is hashed while each process is being approved. The hash code along with the peocess or program name will be stored in the process repository, which will be used by the killer to classify the processes has approved, Malware and unknwn.

User-Management Module: This module supports for registering a new user and authenticating the existing users on their logins. This module will be used by the administrator to manage the user credentials. Building design of the modules

Time Comparisons: We evaluate the execution times of NCD-CEA and the comparative algorithms to confirm the competitive effectiveness of NCD-CEA. Results are acquired by average across all separate runs, with each execution process being free of interruptions from other programmes to ensure precise execution times. All comparison methods mentioned in Section V-A are compatible with the same hardware and programming language. In Tables III and IV, the "Average time" fields display all results. We only displayed the average processing time for the WS100, Ps-contact, Excontact, WS500, Email, and WS1000 networks because the elapsed times of algorithms in the RG100, BA100, and WS100 are nearly comparable. Two statistical findings are presented. 1) As shown in Table III, NCD-CEA solves Hard-EAP occurring in all three networks in the shortest amount of time and defeats other algorithms in solving Easy-EAP in two of the three networks. In Table IV, the benefits of NCD-CEA in lowering the time complexity become increasingly evident as the network scale rises from 500 to 1000. 2) The time costs of NCD-CEA for EasyEAP and Hard-EAP are comparable in small networks, but as the network size grows, Hard-elapsed EAP's time climbs exponentially whereas EasyEAP's elapsed time increases linearly. Both Easy-EAP and Hard-EAP have a solution space of O(2N), where N is the size of the network. As depicted in Fig. 4, in contrast to Easy- EAP's.

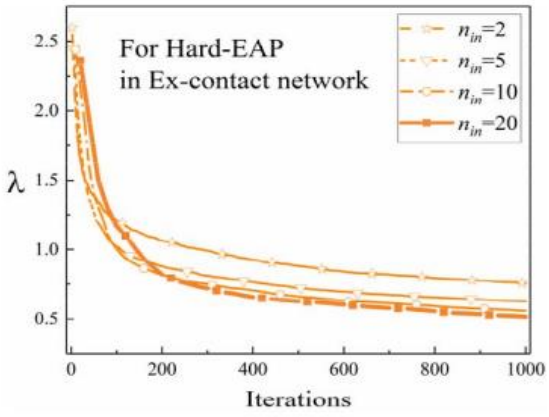

Fig 2: Time Comparision

CONCLUSION AND FUTURE WORK

In this paper, we presented malware detection approach based on class-wise selection of OpCodes sequence as a feature for classification task. A graph of selected features was created for each sample and a deep Eigenspace learning approach was used for malware classification. Our evaluations demonstrated the robustness of our approach in malware detection with an accuracy rate of 98.37% and a precision rate of 98.59%, as well as the capability to mitigate junk code insertion attacks. In the future, we plan to evaluate our approach against larger and broader datasets, and implementing a prototype of the proposed approach in a real-world platform for evaluation and refinement. Furthermore, so as to leverage advantages of distributed computing, the proposed method will redesign somehow efficiently deploy on a network of IoT nodes (e.g. such as the settings described in.

REFERENCES

[1] Priyanka S. Kedar, Vrunda Bhusari, “Using PBKDF2 Pair & Hybrid technique for Authentication”, International Journal of Emerging Research in Management & Technology (ISSN) 2278-9359, Volume-3, Issue-5, May 2014.

[2] M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar, “Authentication Schemes for Session Password using colors and Images”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[3] Priti Jadhao, Lalit Dole, “Survey on Authentication Password Techniques”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[4] Z. Zheng, X. Liu, L. Yin, Z. Liu “A Hybrid password authentication scheme based on shape and text”, Journal of Computers, vol.5, no.5 May 2010.

[5] D.Aruna Kumari, Design, Implementation of Network Based Authentication Mechanisms, Advances in Information Technology and Management, vol.1, no.2, pp.44-48, 2012.

[6] H. Zhao and X. Li, "S3PAS: A Scalable ShoulderSurfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[7] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May2011

[8] D. Aruna Kumari, Design, Implementation of Network Based Authentication Mechanisms, Advances in Information Technology and Management, vol.1, no.2, pp.44-48, 2012.

[9] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy "Authentication Techniques For Engendering Session Passwords With Colors And Text" Advances in Information Technology and Management Vol. 1, No. 2, 2012.

[10]A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42 pp. 41-46, 1999.

[11] L. Sabrado and J. C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002.

[12] L. D. Paulson, "Taking a Graphical Appraoch to the Password," Computer, vol. 35, pp. 19, 2002.

[13] Jean-Camille Birget, Dawei Hong and Nasir Memon, uGraphical Passwords Based on Robust Discretization", IEEE Transactions on Information Forensics and Security, Vol. 1, No.3, September 2006.

[14] L. Y. Por and X. T. Lim, "Multi-Grid background Pass-Go". WSEAS Transactions on Information Science and Applications, Issue 7, Volume 5, July 2008.

[15] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "YAGP: Yet another graphical password strategy". In Annual Computer Security Applications Conference, 2008, 121-129.