A NOVEL APPROACH FOR MODELING AND DETECTION OF CAMOUFLAGING WORM

Vivek Dubale[1], Syed A.H.[2], Kulkarni P.R.[3]

[1] *M.E. Student, Computer Department,Aditya engineering, Maharastra, India*
[2] *Assistant professor, Computer Department, Aditya engineering, Maharashtra, India*
[3] *lecturer, Computer Department, Aditya engineering, Maharashtra, India*

ABSTRACT

The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the C-Worm camouflages its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. We analyze characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and non-worm traffic (background traffic). We observe that these two types of traffic are barely distinguishable in the time domain. However, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, we design a novel spectrum-based scheme to detect the C-Worm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from background traffic. Using a comprehensive set of detection metrics and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based detection scheme.

Keyword: - *C worm,psd,d-dos.*

---

1. INTRODUCTION

In this system, the detection is commonly based on the self propagating behavior of worms that can be described as follows: after a worm-infected computer identifies and infects a vulnerable computer on the Internet, this newly infected computer1 will automatically and continuously scan several IP addresses to identify and infect other vulnerable computers. As such, numerous existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems.

The C-Worm has a self-propagating behavior similar to traditional worms, i.e., it intends to rapidly infect as many vulnerable computers as possible. However, the CWorm is quite different from traditional worms in which it camouflages any noticeable trends in the number of infected computers over time. The camouflage is achieved by manipulating the scan traffic volume of worm-infected computers. Such a manipulation of the scan traffic volume prevents exhibition of any exponentially increasing trends or even crossing of thresholds that are tracked by existing detection schemes .

1.1Existing System.

Existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, 'stealth' is one attack strategy used by a recently-discovered active worm called "Attack" worm and the "self-stopping" worm circumvent detection by hibernating (i.e., stop propagating) with a pre-determined period. Worm might also use the evasive scan and traffic morphing technique to hide the detection.

1.2Proposed System

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work .

In presented a state-space feedback control model that detects and control the spread of these viruses or worms by measuring the velocity of the number of new connections an infected computer makes. Despite the different approaches described above, we believe that detecting widely scanning anomaly behavior continues to be a useful weapon against worms, and that in practice multifaceted defense has advantages.

2. LITERATURE SURVEY

Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

Active worms are similar to biological viruses in terms of their infectious and self-propagating nature. They identify vulnerable computers, infect them and the worm-infected computers propagate the infection further to other vulnerable computers. In order to understand worm behavior, we first need to model it. With this understanding, effective detection and defense schemes could be developed to mitigate the impact of the worms. For this reason, tremendous research effort has focused on this area,

Active worms use various scan mechanisms to propagate themselves efficiently. The basic form of active worms can be categorized as having the Pure Random Scan (PRS) nature. In the PRS form, a worm-infected computer continuously scans a set of random Internet IP addresses to find new vulnerable computers. Other worms propagate themselves more effectively than PRS worms using various methods, e.g., network port scanning, email, file sharing, Peer-to-Peer (P2P) networks, and Instant Messaging (IM. In addition, worms use different scan strategies during different stages of propagation. In order to increase propagation efficiency, they use a local network or hit list to infect previously identified vulnerable computers at the initial stage of propagation. They may also use DNS, network topology and routing information to identify active computers instead of randomly scanning IP addresses. They split the target IP address space during propagation in order to avoid duplicate scans. Studied a divide-conquer scanning technique that could potentially spread faster and stealthier than a traditional random-scanning worm. Ha formulated the problem of finding a fast and resilient propagation topology and propagation schedule for Flash worms. Studied the worm propagation over the sensor networks

Worm (C-Worm) studied in this paper aims to elude the detection by the worm defense system during worm propagation. Closely related, but orthogonal to our work, are the evolved active worms that are polymorphic in nature. Polymorphic worms are able to change their binary representation or signature as part of their propagation process. This can be achieved with self-encryption mechanisms or semantics preserving code manipulation techniques. The C-Worm also shares some similarity with stealthy port-scan attacks. Such attacks try to find out available services in a target system, while avoiding detection. It is accomplished by decreasing the port scan rate, hiding the origin of attackers, etc. Due to the nature of self-propagation, the C-Worm must use more complex mechanisms to manipulate the scan traffic volume over time in order to avoid detection.

3. SYSTEM ANALYSIS.

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple.

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. Select methods for presenting information.Create document, report, or other formats that contain information produced by the system.

4.FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

4.1 Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

4.2Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

4.3Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

5.SYSTEM DESIGN

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

5.1Data Flow Diagram / Use Case Diagram / Flow Diagram

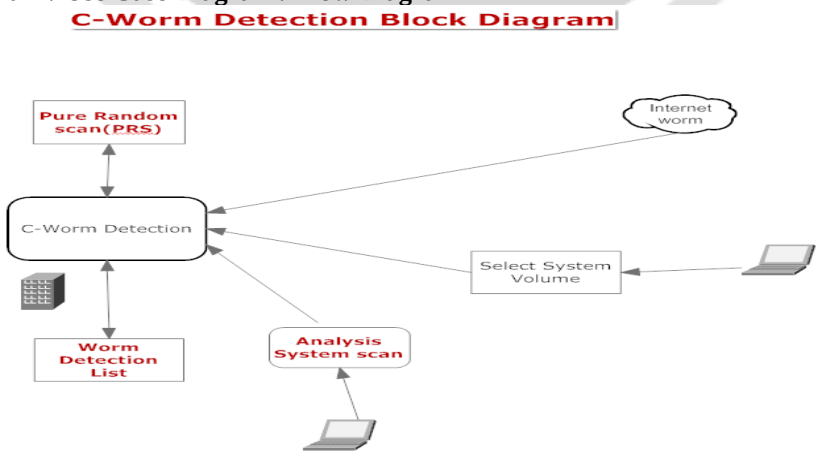

Fig 5.1 C worm detection block diagram

5.2 UML Design

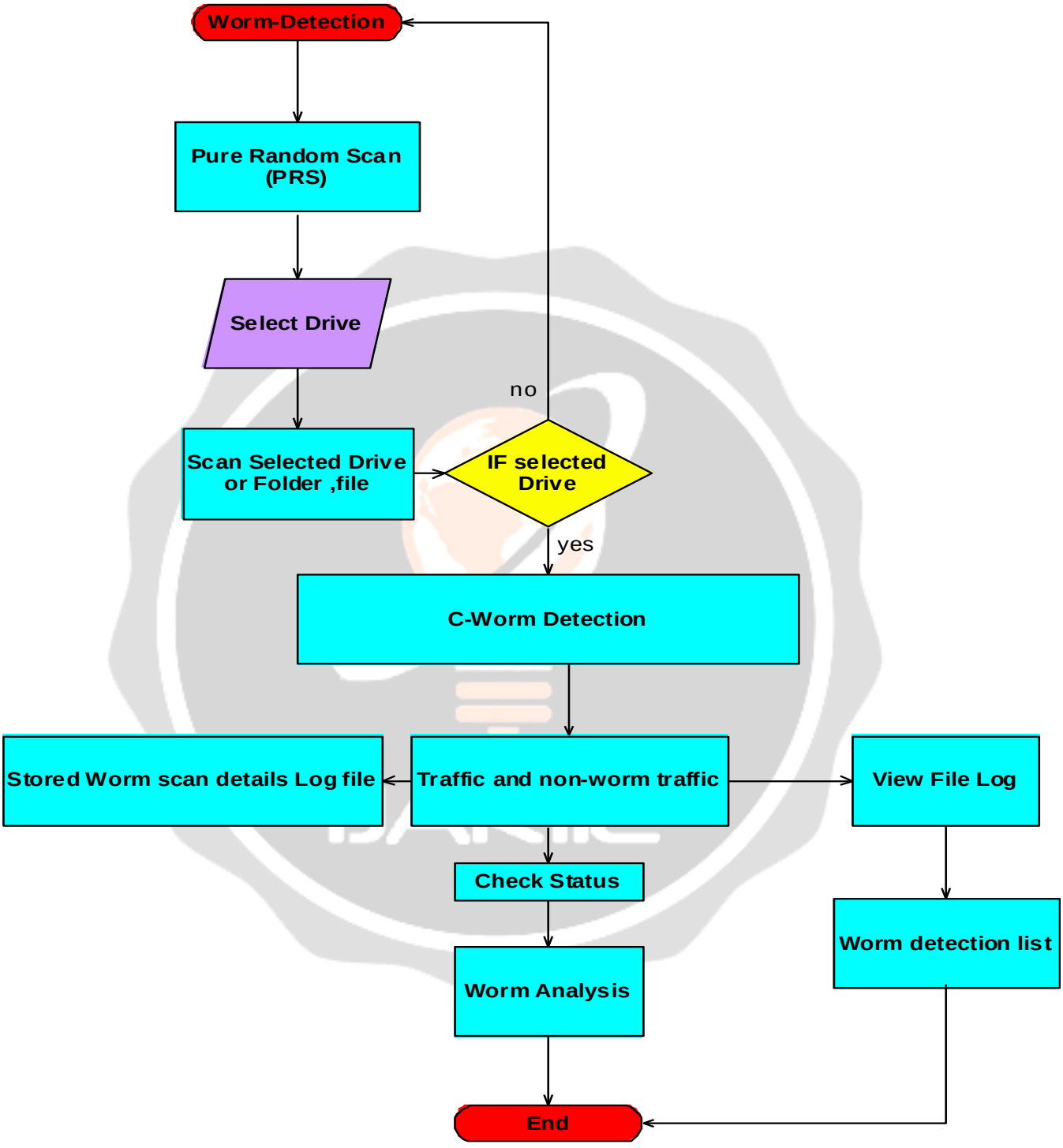

Fig 5.2 C worm detection block diagram

5.3 Activity Diagram

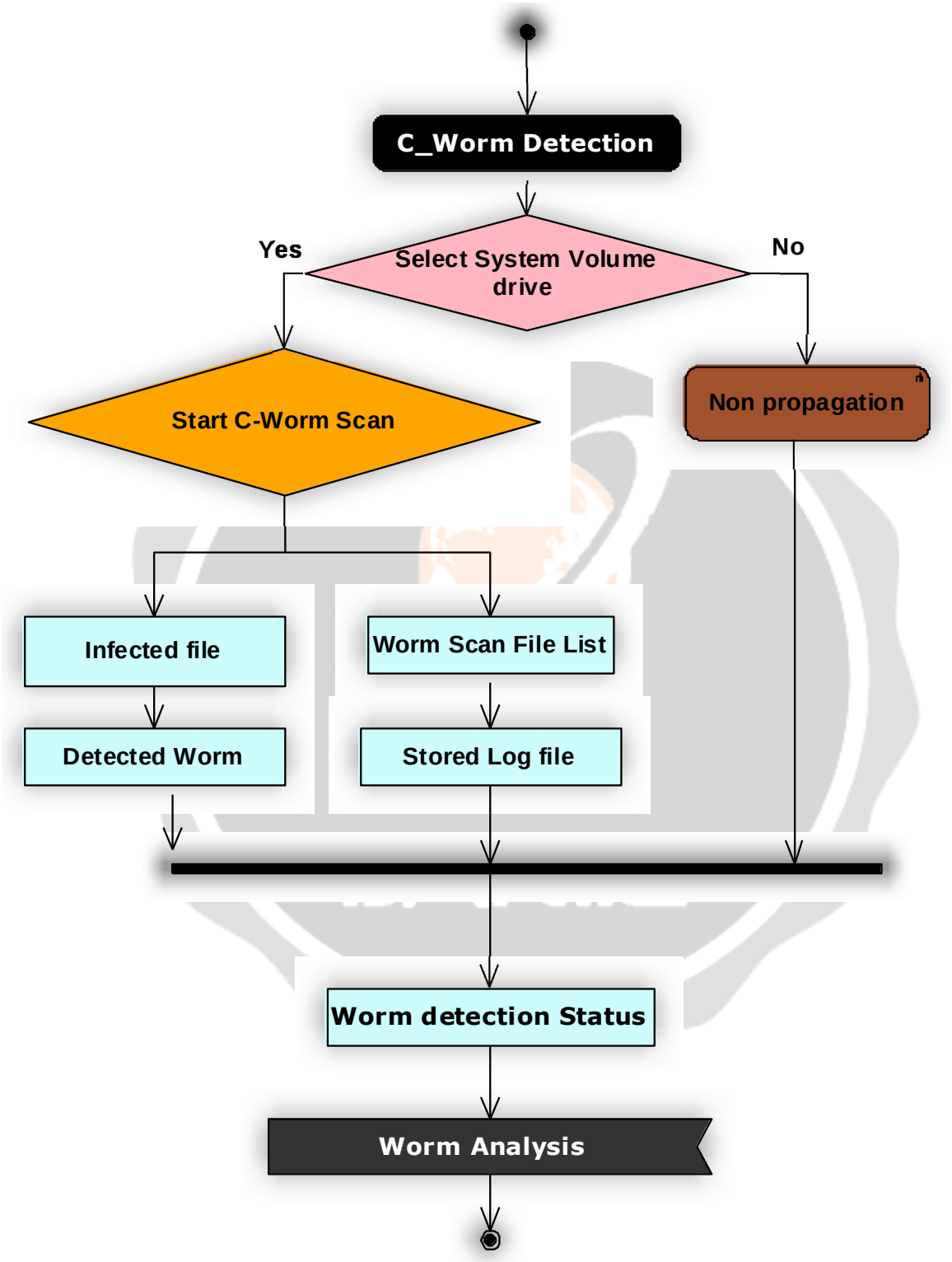

Fig 5.3 Activity Diagram

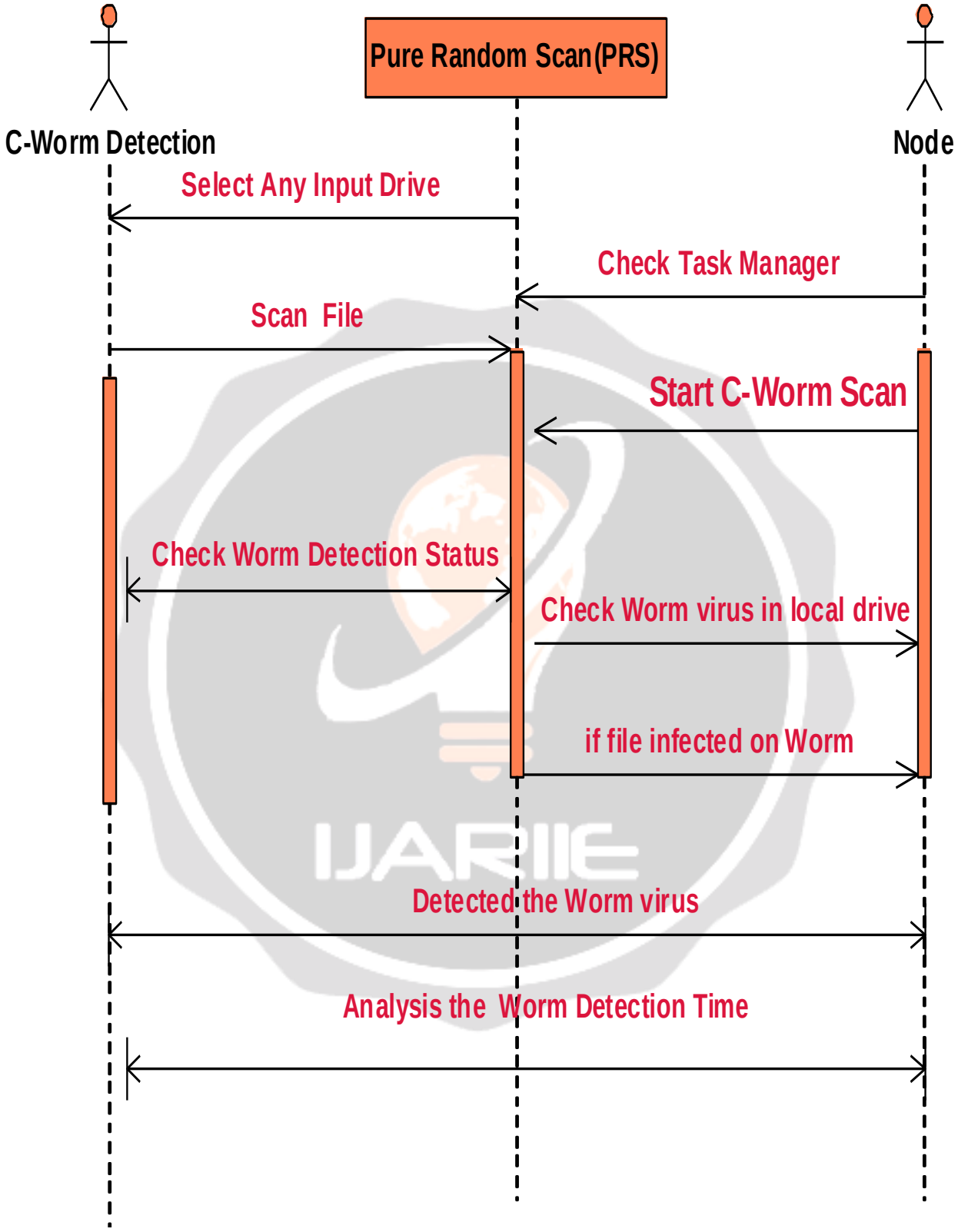

Fig 5.4 Source Diagram

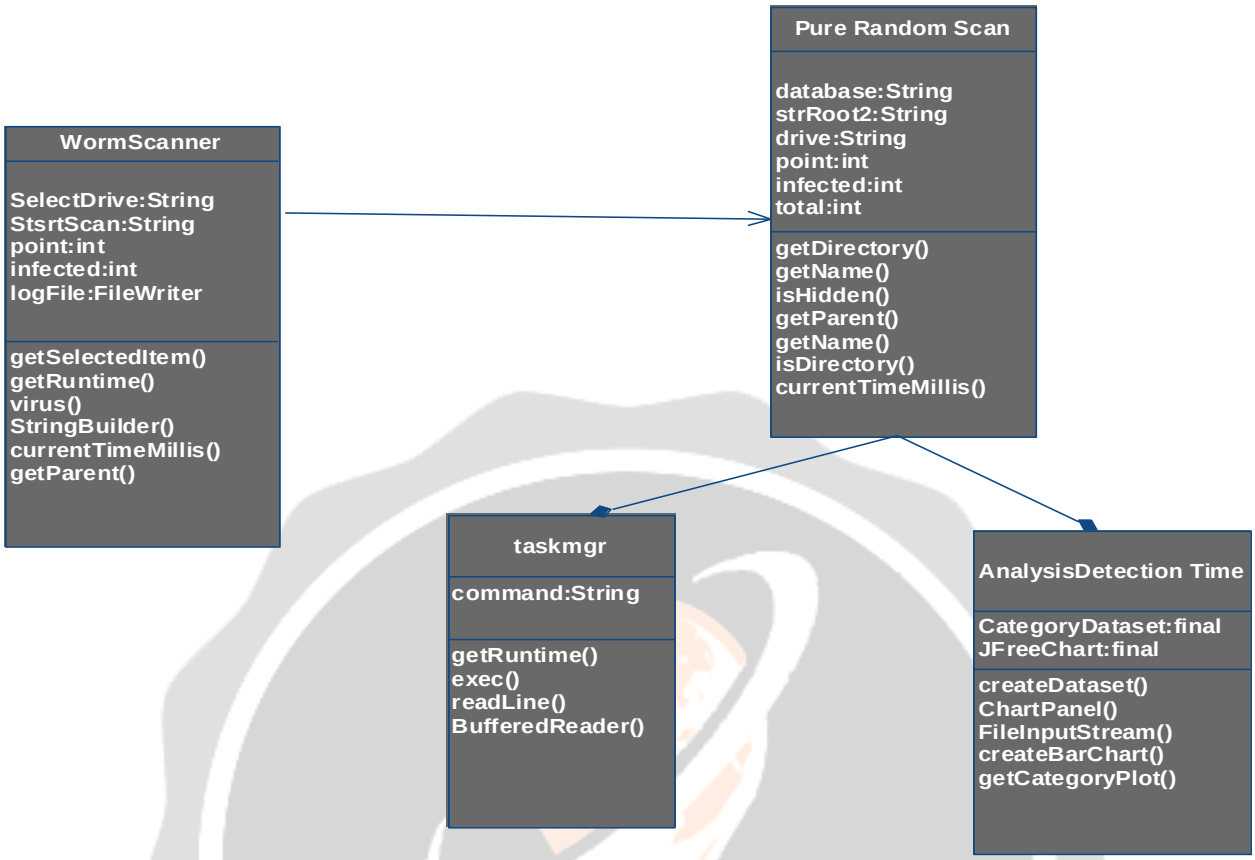

Fig 5.5 Class Diagram

6. OUTPUT SCREEN

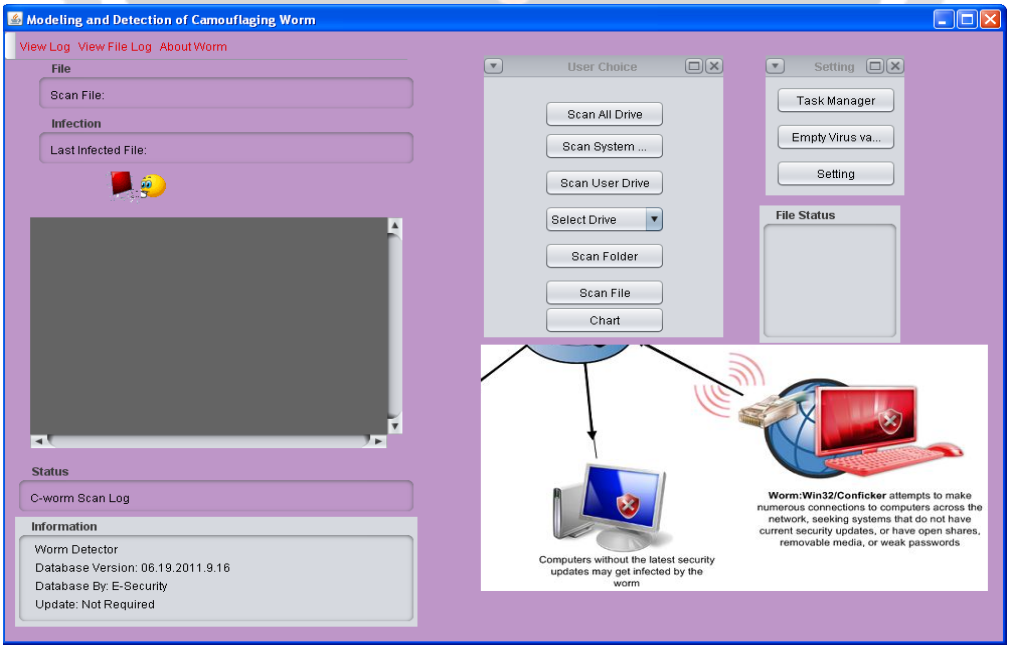

Fig 6.1 Output Screen

7.SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

4. CONCLUSIONS

This is how we can implement the system for Modeling and Detection of Camouflaging Worm and we can overcome the problems with the existing system like Existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, 'stealth' is one attack strategy used by a recently-discovered active worm called "Attack" worm and the "self-stopping" worm circumvent detection by hibernating (i.e., stop propagating) with a pre-determined period. Worm might also use the evasive scan and traffic morphing technique to hide the detection.

REFERENCES

[1] D. Moore, C. Shannon, and J. Brown, "Code-red: a case study on the spread and victims of an internet worm," in Proceedings of the 2-th Internet Measurement Workshop (IMW), Marseille, France, November 2002.

[2] D. Moore, V. Paxson, and S. Savage, "Inside the slammer worm," in IEEE Magazine of Security and Privacy, July 2003.

[3] CERT, CERT/CC advisories, http://www.cert.org/advisories/.

[4] P. R. Roberts, Zotob Arrest Breaks Credit Card Fraud Ring, http: //www.eweek.com/article2/0,1895,1854162,00.asp.

[5] W32/MyDoom.B Virus, http://www.us-cert.gov/cas/techalerts/ TA04 028A.html.

[6]W32.Sircam.Worm@mm,http://www.symantec.com/avcenter/venc/data/ w32.sircam.worm@mm.html.

[7]Worm.ExploreZip,http://www.symantec.com/avcenter/venc/data/wo m.explore.zip.html.

[8] R. Naraine, Botnet Hunters Search for Command and Control Servers, http://www.eweek.com/article2/0,1759,1829347,00.asp.

[9] T. Sanders, Botnet operation controlled 1.5m PCs Largest zombie army ever created, http://www.vnunet.com/vnunet/news/2144375/ botnet-operation-ruled-million, 2005.

[10] R. Vogt, J. Aycock, and M. Jacobson, "Quorum sensing and selfstopping worms," in Proceedings of 5th ACM Workshop on Recurring Malcode (WORM), Alexandria VA, October 2007.

[11] S. Staniford, V. Paxson, and N.Weaver, "How to own the internet in your spare time," in Proceedings of the 11-th USENIX Security Symposium (SECURITY), San Francisco, CA, August 2002.

[12] Z. S. Chen, L.X. Gao, and K. Kwiat, "Modeling the spread of active worms," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.

[13] M. Garetto, W. B. Gong, and D. Towsley, "Modeling malware spreading dynamics," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.
[14] C. C. Zou, W. Gong, and D. Towsley, "Code-red worm propagation modeling and analysis," in Proceedings of the 9-th ACM Conference
on Computer and Communication Security (CCS), Washington DC, November 2002.
[15] Zdnet, Smart worm lies low to evade detection, http://news.zdnet.co.uk/ internet/security/0,39020375,39160285,00.htm.
[16] J. Ma, G. M. Voelker, and S. Savage, "Self-stopping worms," in Proceedings of the ACM Workshop on Rapid Malcode (WORM), Washington D.C, November 2005.
[17] Min Gyyng Kang, Juan Caballero, and Dawn Song, "Distributed evasive scan techniques and countermeasuress," in Proceedings of International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA), Lucerne, Switzerland, July 2007.