International **J**ournal of **S**oft **C**omputing and **S**oftware **E**ngineering (**JSCSE**)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

Development, Implementation and Performance Evaluation of the Optimal Anti-Worm Detection Defense Software (OAWDDS) Protocol

*** Dr.Carol A. Niznik**
NW SYSTEMS
Rochester, N.Y., U.S.A.

Abstract. Computer Worms known as malicious codes are defined as programs that replicate without infecting other programs and some Worms spread by copying themselves from disk to disk or computer to computer across a network, while others replicate in memory to slow the computer. There are five components of a Worm and the individual Worm nodes can be linked in a communication network to build a larger Worm network with five topologies. The five Worm network topologies are: Hierarchical Tree, Centrally Connected, Shockwave Rider-Type, Hierarchical Tree with Several Layers of Authority and Many Centralized Nodes,and Full Mesh. The Optimal Anti-Worm Detection Defense Software(OAWDDS)Protocol realizes three optimization constraints from the mathematical formalization of a Worm: five components, five topologies, and five structures. The computer networking Queueing System Modeling of the exponential Worm growth characteristics with GI/G/1, M/M/1,and E2/M/1 Queueing Parameters within the three constraints and formed computer network congestion control between possible Worm Hosts and Worm Nodes will ensure 100% elimination of Worm Network protection. The analytical Lagrangian optimization in the OAWDDS Protocol of the proportion of vulnerable machines compromised with the three constraints will ensure the following three criteria to be enforced: (A)stopping Worm attacks 100% of the time,(B)enabling 100% protection for a given system without knowing any of the signatures of the individual Worms and (C)maintaining 100% effectiveness without periodic updates like virus protection. These three criteria will assure critical government public and private infrastructure systems required to maintain the national and economic security of the U.S.

Keywords: *anti-worm, worm networks, 5 worm network topologies, OAWDDS Protocol, worm growth.*

* Corresponding Author:

Dr. Carol A. Niznik,
NW SYSTEMS, Rochester, N.Y., U.S.A

Email: Email: dr_carol-niznik@yahoo.com

1. Introduction

Worms are defined as programs that replicate without infecting other programs and some Worms spread by copying themselves from disk to disk or computer to computer across a network while others replicate only in memory to slow the computer. Computer Worms known as malicious codes are defined as programs that replicate without infecting other programs and some Worms spread by copying themselves from disk to disk or computer to computer across a network, while others replicate in memory to slow the computer. Therefore, a worm exploits security flaws in computers on the network. With the development of network applications worms can exploit various ways to propagate themselves quickly. The spread of worms is much faster than human beings can manually respond. Thus worms are becoming more and more stealthy with the adoption of polomorphism and metamorphism techniques[17,20,21].

A Worms life consists of the following phases: target finding, transferring, activation, and infection. Worms involve network activities in the first two phases for the developing detection algorithms. The OAWDDS Protocol developed realizes detection and containment systems. After detecting the existence of Worms a containment must be realized by the software protocol. Worm characteristics during target finding and Worm transferring phases are realized. The worm defense mechanisms of detection and containment are implemented.

International **J**ournal of **S**oft **C**omputing and **S**oftware **E**ngineering (**JSCSE**)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

The following are definitions of worm characteristics[16]:
(1) Activation occurs when a worm starts performing malicious activities on a specific date or under certain conditions.
(2) False alarm is an incorrect alert generated by a worm detection saystem.
(3) False Positive is a false alarm where an alert is generated when there is no actual attack or threat.
(4) False Negative means the detection indicates a system misses an attack if no alert is generated while the system is under attack.
(5) Infestation is the result of the worm performing its malicious activities on the host[12].
(6) Target finding is the first step in a worm's life to discover victims(vulnerable hosts)[3].
(7) Threshold is a predefined condition that if met, indicates the existence of specious traffic or a worm attack[1,2,17].
(8) Transfer refers to sending a copy of the worm to the target after the victim(target) is discovered[8].
(9)Virus is a malicious piece of code that attaches to other programs to propagate[24]. The virus cannot propagate by itself and depends on certain user intervention.
(10) A Passive worm only propagates itself until it is contacted by another Host.

Figure 1 18 Section Geometric Software Structure For The Worm Definition Parameters

2. Mathematical Definition of a Worm

A Worm is defined by the following mathematical statement,

<R,At,Co,Cd,I,Ht,Cn,SR,Hn,Fm,Tp,Vs,L,St,Pdm,M,t,T> **(1)**

A Worm can be mathematically formalized as the 18 tuple, realizing the five components, five topologies, and five structures [18]:

The five components of a Worm are:
(R) Reconnaissance, and four components,

International **J**ournal of **S**oft **C**omputing and **S**oftware **E**ngineering (**JSCSE**)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

(A) Attack,
(Co) Communication,
(Cd) Command, and
(I) Intelligence.
Individual Worm nodes can be linked in a communication network to build a larger Worm network with five topologies,
(Ht) Hierarchical tree,
(Cn) Central net,
(SR) Shock wave Rider,
(Hn) Hierarchical net, and
(Fm) Full mesh
five Worm structures:
(Tp) Target platform,
(Vs) Vulnerability selection,
(L) Language,
(St) Scanning technique and
(Pdm) payload delivery mechanism enabling
M the proportion of vulnerable machines compromised.
t = time
T = a constant at which growth of the Worm began.
Refer to Figure 1 for an 18 Section Geometric Software Structure For The Worm Definition Parameters.

There are five components of a Worm and the individual Worm nodes can be linked in a communication network to build a larger Worm network with five topologies. The five Worm network topologies are: Hierarchical Tree, Centrally Connected, Shockwave Rider-Type, Hierarchical Tree with Several Layers of Authority and Many Centralized Nodes,and Full Mesh. Refer to Figure 2 A,B.C,D,E for these Worm Topologies.

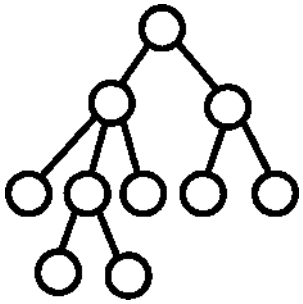

Figure 2.A Network Topology Hierarchical Tree

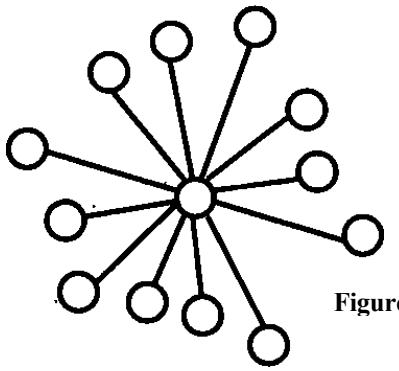

Figure 2.B Network Topology Centrally Connected Network

International Journal of Soft Computing and Software Engineering (JSCSE)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

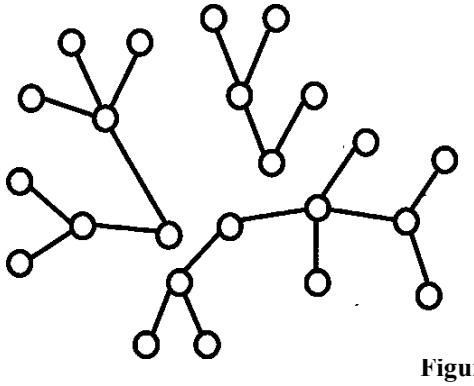

Figure 2.C Network Topology Shockwave Rider-Type of Network

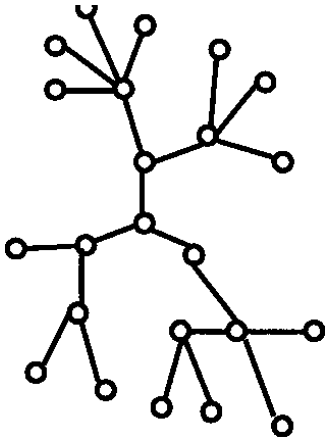

Figure 2.D Network Topology Hierarchical Tree Several Layers of Authority and Many Centralized Nodes

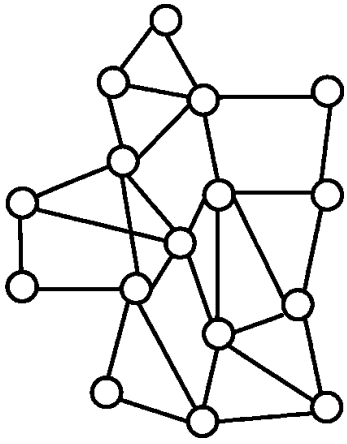

Figure 2.E Network Topology Full Mesh Topology

Figure 2 WORM Network With Five Topologies

International Journal of Soft Computing and Software Engineering (JSCSE)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

3. OAWDDS Protocol Derivation

The Optimal Anti-Worm Detection Defense Software(OAWDDS)Protocol realizes three optimization constraints from the mathematical formalization of a Worm: five components, five topologies, and five structures[1,2]. Worms using rapid scanning strategies realize an exponential formalism at the beginning of their growth and slow down as they attempt to infect the same nodes over and over. The computer networking Queueing System Modeling[10,11] of the exponential Worm growth characteristics with GI/G/1, M/M/1,and E2/M/1 Queueing Parameters, within the three constraints and formed computer network congestion control between possible Worm Hosts and Worm Nodes will ensure 100% elimination of Worm Network protection.

The analytical Lagrangian optimization in the OAWDDS Protocol of the proportion of vulnerable machines compromised with the three constraints will ensure the following three criteria to be enforced: (A) stopping Worm attacks 100% of the time,(B) enabling 100% protection for a given system without knowing any of the signatures of the individual Worms and (C) maintaining 100% effectiveness without periodic updates like virus protection. These three criteria will assure the critical government public and private infrastructure systems required to maintain the national and economic security of the United States[21,22,23,24].

The analytical Lagrangian optimization[14] of the proportion of vulnerable machines compromised **M**[6,7] requires constraints based on the five topologies, five components and five structures[18]. The OAWDDS Protocol Development and Performance Analysis will ensure the criteria described by A, B, and C described in the following equations[4]:

$$\mathbf{M} = [\ \varepsilon^{K(t-T)}\ ] / [1+ \varepsilon^{K(t-T)}\ ] \qquad (2)$$

where,
K = the initial compromise rate, which is scaled to account for
machines already infected,
t = time, and
T is a constant at which growth of the Worm began.

This Worm growth characteristic in computer networking is mathematically described as the M/M/1 Queueing system. The optimized value for the proportion of vulnerable machines **OM** required[8,13,15] to attain criteria **A, B** and **C** will be realized based on:

$$\mathbf{OM = M + \alpha [\ Comp - P1\ ] + \beta [\ Top - P2\ ] + \lambda [\ Struc - P3\ ]} \qquad (3)$$

where,
α = Worm Component constraint Lagrange multiplier,
P1 = Worm Component Constraint,
β = Worm Topology Constraint Lagrange Multiplier**,**
P2 = Topology Constraint**,**
λ = Worm Structural Constraint Lagrange Multiplier**,**
P3 = Worm Structural Constraint.
OM = 0 to achieve **(A)**, **(B)** and **(C)**. The Lagrangian optimization of eqn**.(3)** requires the following solution for the Lagrange Multipliers **α, β,** and **λ,** and their solution substitution into eqn **(3)** with **OM** = 0 to obtain **OM**, **Comp**, **Top** and **Struc** for constraints **P1**,**P2**,**P3**.

$$\partial \mathbf{OM}/\alpha = 0, \qquad (4)$$

$$\partial \mathbf{OM}/\beta = 0, \qquad (5)$$

$$\partial \mathbf{OM}/\lambda = 0 \qquad (6)$$

Each of the two hexagonal OAWDDS Protocol object oriented code geometric structures face each other via their placement on a folding two sided screen, whose sides each contain one of the two OAWDDS Protocol geometric hexagonal structures. The first OAWDDS Protocol geometric hexagonal structure contains the five Worm Components sides with the Detection property on the sixth side facing the other hexagonal geometric structure. The second hexagonal geometric software structure for the OAWDDS Protocol contains the five Worm Structures on the five sides and the Defense property on the sixth side. The OAWDDS Protocol in its object oriented software code realizes equation **(3)** to prevent Worm Hosts from forming and the

International **J**ournal of **S**oft **C**omputing and **S**oftware **E**ngineering (**JSCSE**)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

Topological Worm networks, which would enable infrastructure deadlock. Refer to Figure 3 for the Hexagonal OAWDDS Protocol Geometric Structures.

Additional Queueing System Software Modeling of the exponential growth with GI/G/1, M/M/1, and E2/M/1 Queueing Models parameters within the three constraints and formed computer network congestion control and gateway software criteria, between possible Worm Hosts and Worm Nodes will be realizes within the OAWDDS Protocol to ensure the 100% elimination of the Worm network protection and prevention of deadlock and livelock. Refer to Figure 4 for the Flow Chart of the OAWDDS Protocol Development and Performance Analysis. The Anti-Worm System OAWDDS Protocol can be processed on a standard Windows platform (laptop, desktop or server) with any currently supported Windows operating system.

4. Summary

Some of the most obvious techniques exhibited by Worms are to find widespread security holes in a network and increase their scanning rate. A secure network[2,3,22] is composed of firewalls, sensors, analyzers honeypots and various scanners and probes. The **OADDS** Protocol Software developed here will therefore provide a secured network because of its Geometric Mathematical formalism basis and its characterization of the properties necessary to stop Worm growth and infestation in networks[12].

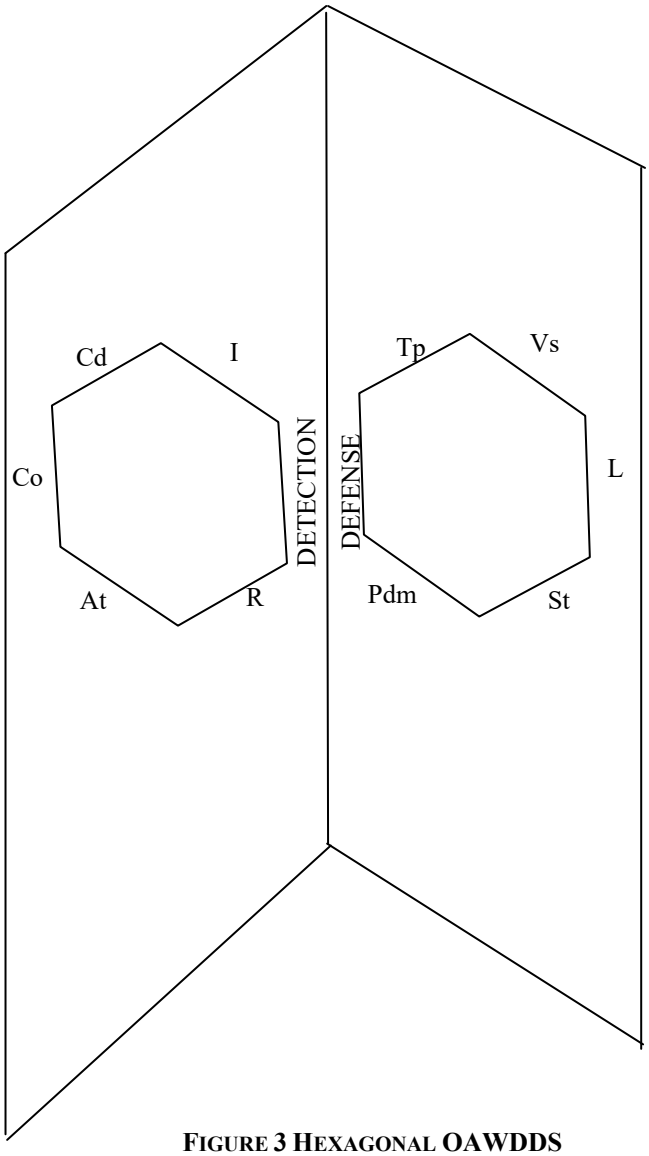

FIGURE 3 HEXAGONAL OAWDDS GEOMETRIC STRUCTURES

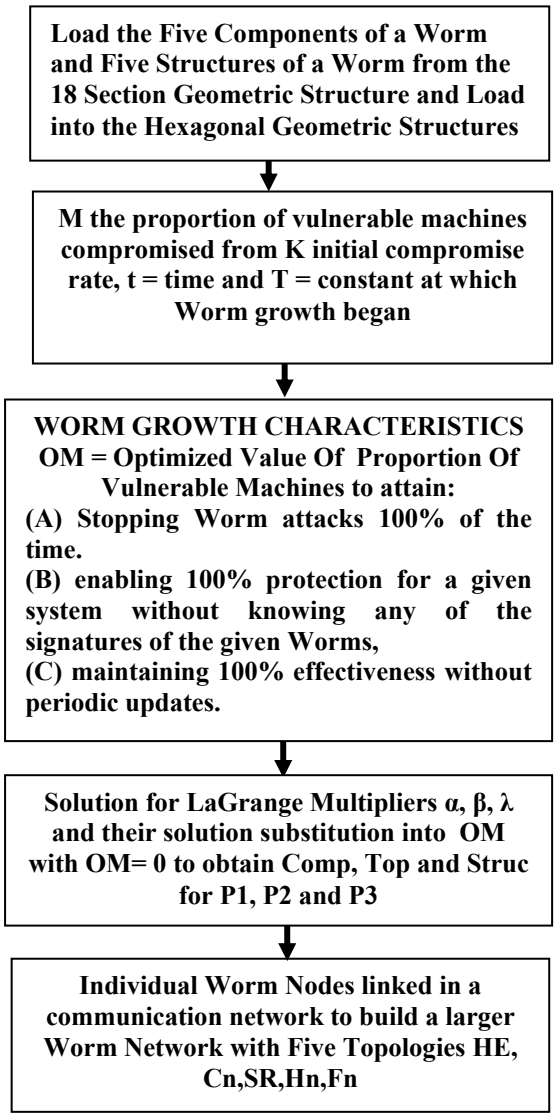

FIGURE 4 OAWDDS THEORETICAL DEVELOPMENT AND PERFORMANCE ANALYSIS

International **J**ournal of **S**oft **C**omputing and **S**oftware **E**ngineering (**JSCSE**)
Vol.5, No.5, 2015

Published online: May 25, 2015

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v5.n5.1

ACKNOWLEDGEMENT
The Author acknowledges the geometric structure for Figure 1 from the structure of the Rose Window In The West Front at the Nadros Cathedral in Trondheim, Norway[18].

REFERENCES

[1] G.B.V.Berk and Morris,"Designing a Framework for Active Worm Detection on Global Networks",Proc. 1st IEEE Int'l Wksp. Info. Assurance, 2003.
[2] L.-H.D. David Brumley, Pongsin Poosankam, and Dawn Song, "Design Space and Analysis of Worm Defense Strategies ",Proc. ACM Symp.Info.Comp. and Commun. Sec.. 2006.
[3] Z. Chen, L. Gao, K.Kwiat,"Modeling the Spread of Active Worms, Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'2003), SanFrancisco, CA.,U.S.A., Mar.2003, pp. 1890-1900.
[4] S. Chen, Y. Tang, "DAW A Distributed Anti-Worm System", IEEE Trans.Parallel Distrib. Syst. Vol. 18, no.7, pp. 893-906, 2007.
[5] S. Chen, Y. Tang,"Slowing Down Internet Worms", Proceedings of the 24th International Conference on Distributed Computing Systems(ICDCS'04), pp.1-8.
[6] R. Dantu, J. Cangussu, A. Yelimeli, "Dynamic Control Of Worm Propagation", Proc.International Conference On Information Technology, Coding and Computing (ITCC'04), vol. 1, 2004.
[7] R.V. Dantu, "An Architecture of Security Engineering" Proc.ACSA Workshop on Application of Engineering Principles for Security System Design, November 2002.
[8] M.S.G.Gu et.al., "Worm Detection, Early Warning and Response Based on Local Victim Information", Proc. 20th Annual Comp.Sec. Apps. Conf. 2004.
[9] K. Iigun, R. Kemmerer,and P.Porras, "State Transition Analysis: A Rate Based Intrusion Detection Approach," IEEE Trans. Software Eng., vol. 2, pp.181-199, 1995.
[10] L. Kleinrock, Queueing Systems: Computer Applications, John Wiley and Sons, 1976.
[11] L. Kleinrock, Queueing Systems: Theory, John Wiley Publishers, 1975.
[12] M. Liljenstam, Y. Yuan, B. Premore, and D. Nicol, "A Mixed Abstraction Level Simulation Model of Large- Scale Internet Infestation", Proc .of 10th IEEE/ACM Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, (MASCOTS), October 2002.
[13] B.M.J. Lockwood, "Design of a System for Real-Time Worm Detection", Proc.12th IEEE Annual Symp.High Perf. Inter-Connects,2004.
[14] C.A. Niznik, Measures of Congestion for Computer Communication Networks, PhD Dissertationm, SUNY at Buffalo, June, 19778.
[15] D.D.X. Quin et al., "Worm Detection Using Local Networks", tech.rep. College of Computing, Georgia Tech.
[16] P. Li, M. Salour, X. Su, "A Survey Of Internet Worm Detection And Containment", IEEE Communications Surveys & Tutorials, 1st Quarter 2008, vol.10,No.1,pp 20-35.
[17] S. Singh, C. Estan, G. Vargese, and S. Savage, "The Early Bird System for Real-Time Detection of Unknown Worms", Proc.Sixth Symp. Operating System Design and Implementation(OSDI'04), Dec. 2004.
[18] T.F. Suul, Nidaros Cathedral The Stained Glass Window Published by Nidros Domimkirkes Restaureringsarbeider, Translated by Micheal Stevens, 1983.
[19] Y. Tang, S. Chen," Defending Against Internet Worms; A Signature-Based Approach", INFOCOM 2005 24th Annual Joint Conference of the IEEE Computer and Communications Societies , Proc. IEEE, vol. 2, March 13-17, 2005.
[20] Y. Tang, S. Chen,"Inside the Permutation-Scanning Worms: Propagation Modeling and Analysis",IEEE/ACM Trans.On Networking, vol.18, no. 3,6/2010, pp.85-870.
[21] Y. Tang, J, Luo, B. Xiao, G. Wei, "Concept, Characteristics And Defending Mechanisms of Worms", IEICE Trans. Inf. & Syst. vol.E92-D, no.5, May 2009, pp.799-809.
[22] W. Wu, S.Vangala,L.Gao, and K.Kwait, "An efficient Architecture and algorithm for detecting worms with various scan techniques.", in Proceedings of the 11thAnnual Network and Distributed Sytem Security Symposium (NDSS'04), February, 2004.
[23] V.P.N. Weaver, S.Saniford and R.Cunningham, "A Taxonomy of Computer Worms",Proc.ACM WORM'03, 2003.
[24] M.M. Williamson, "Throttling Viruses: Restricting Propagation to Defeat Malicious Code ", Proc. 18th Ann. Computer Society Application Conf. (ACSAC'02), Dec 2002.