CHEMICAL ENGINEERING TRANSACTIONS
VOL. 51, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Tichun Wang, Hongyang Zhang, Lei Tian
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-43-3; **ISSN** 2283-9216
DOI: 10.3303/CET1651133

Radiation-Based Virus Attack and Defense Reliability Optimization Design

Peng Yang

Department of Information Engineering, ShaanXi Polytechnic Institute, Xianyang, Shaanxi 712000, China
ypeng1123@sina.com

In this paper, the feasibility of computer networks against virus attacks are analyzed, pointing out the characteristics of computer virus weapon, injection methods and attacks. The last of a computer virus spread in the network established a relevant mathematical model. From the simulation results, we can see a computer spread of the virus in the network speed and the number of infected machines varies with time, so as to implement computer virus attacks radiation information provided strong evidence. A computer virus attack and defense model of radiation information, the establishment of the virus, through the network communication protocol analysis. The original virus information are coded modulation corresponding conversion, so the network can recognize the enemy and running, then fired out through radio, after field line coupling mode, enter the enemy network.

1. Introduction

With the development and improvement of computer technology, there has been able to pose a serious threat to computer security computer viruses (Balog 2007). It stumbled from the initial research until the targeted destruction of computer network information security becomes a major risk (Seager, 2012). Currently, computers are widely used in various sectors, security and computer invasion of viruses will become a means of struggle, greatly improve the ability of computer network attack and defense, high-tech conditions, which is an effective way of information confrontation (Li and Szekely, 2014). The computer network is the computer technology and communication technology closely integrated product, used in modern electronic systems has become increasingly common, and its importance has become increasingly prominent (Site, 2015). Security is a major issue of the current research computer network, network security involves two aspects: First, the performance of defense, namely the security and confidentiality of network information and network against malicious interference, especially the anti-virus attack capability; the second is to attack the performance, which is important for certain hostile network attacks capacity (Programme, 2016).

The early 1920s, the reliability issue has just been raised, people question the reliability of the image of the lack of awareness (Tu, 2012). Until the outbreak of the Second World War, a large number of new weapons and equipment into the battlefield which, in a brutal war environment, many weapons unreliable weapons to the user to bring a painful lesson (Balog, 2006). War countries have begun to attach importance to the reliability of weapons and equipment, and after the war extended to other industries and fields (Arnason, 2015). Thus, the study of the reliability problem is that people gradually groped in practice, for it is the inevitable result of the study of science and technology development to a certain extent after (Ramana, 2016). After long-term development, and reliability issues related to the subject more and more areas, and gradually formed a new comprehensive interdisciplinary (Kuzushima and Tang, 2013).

In this paper, the key technologies of computer network radiation information attack and defense had a full and detailed study to solve the computer virus information radiation attack and defense mechanism, radiation injection computer virus information, security, wired recognition technology computer virus information, computer network antivirus radiation attack key technical protection radius, according to research, computer network virus attack and defense radiation information mechanistic detailed theoretical analysis, it helps to understand the information against the principle behind the smooth start of the program designed to lay a solid foundation. A computer virus attack and defense model of radiation information, the establishment of the virus,

Please cite this article as: Yang P., 2016, Radiation-based virus attack and defense reliability optimization design, Chemical Engineering Transactions, 51, 793-798 DOI:10.3303/CET1651133

through the network communication protocol analysis, the original virus information are coded modulation corresponding conversion, so the network can recognize the enemy and running, then fired out through radio, after field line coupling mode, enter the enemy network.

2. The related theory and method

2.1 Computer network reliability algorithm

Complete state enumeration method, algorithm and do not pay, inclusion and exclusion algorithm, factorization algorithms, special network belong to the traditional algorithm computer network reliability. Wherein the complete state enumeration method since the method is simple, it is widely used in the computer network reliability.

The main idea of the state of enumeration method solve the network reliability by enumerating all the networks mutually exclusive events under specified conditions of normal operation, Bj to calculate the reliability of the network. Network reliability is given by:

$$R_e = \sum^{m} P\left(B_i\right) \tag{1}$$

GA is not strictly limited to the scope and type of objects, especially for the complicated system related to the deconstruction of the most reasonable solution input method is reasonable and easy to row. Establish standard procedures given below genetic algorithms for solving specific problems and get the most optimized solution provides a standard method.

Fitness value selection function give to a range of cost-value coding (the maximum is set to Pop-size; the minimum is set to 1), and re-set in descending order according to the individual cost values, the purpose of this work is to choose the algorithm process deviations may occur Ideally restrictions, this fitness function can be expressed as follows build:

$$f\left(x\right) = \frac{x-1}{PoP\_size-1} \tag{2}$$

2.2 Mathematical model of the network virus transmission

Computer virus attacks on the network is to use the characteristics of the virus infection, when we LAN to a computer virus injection is successful, the virus transmitted through large-scale information and communication on the LAN, a certain trigger condition is satisfied after the virus began to proceed damaging effects, so as to meet the LAN computer virus attack requirements.

M secondary data communication within the n-th unit time and the n + 1 units of time gap, the source machine infected machine mathematical expectation is:

$$\frac{M}{N} E\left(x_n\right) \tag{3}$$

The number of non-toxic target machine mathematical expectation:

$$M - \frac{M}{N} E\left(x_n\right) \tag{4}$$

Roots dig assumptions and random spread of new mathematical expectation of increased exposure of the machine as follows:

$$\frac{M}{N} E\left(x_n\right)\left(1 - \frac{E\left(x_n\right)}{N}\right) \tag{5}$$

So this time the number of infected machines is:

$$E\left(x_{n+1}\right) - E\left(x_n\right) = \frac{M}{N} E\left(x_n\right)\left(1 - \frac{E\left(x_n\right)}{N}\right) \tag{6}$$

Per unit time the number of infected machines is:

$$\frac{E\left(x_{n+1}\right)-E\left(x_n\right)}{\left(n+1\right)-n}=\frac{M}{N}E\left(x_n\right)\left(1-\frac{E\left(x_n\right)}{N}\right) \tag{7}$$

Because, f (0) = 1, the number of computers infected at the time of:

$$E\left(x_n\right)=\frac{N}{\left[1+\left(N-1\right)e^{\left(-\pi M/N\right)}\right]} \tag{8}$$

Computer network communications to maintain a certain density, we choose a strong infectious virus attack, when the spread of the virus to a certain extent, they stimulate the virus triggering module destruction, thus completing the network virus attacks.

2.3 The establishment of the virus database

We chose virus attacks, is that it has a computer network attack characteristics, with the continuous development of virus technology, with different targets and performance viruses are emerging. In accordance with the operating system to attack the virus, we have established the virus for windows operating system.

Police virus: it is designed to detect enemy computer systems, and proven performance characteristics of their systems, computer monitor arms reconnaissance, jamming and other military operations from the enemy, such as: "spy-type" virus, Figure 1 shows part of the virus code packet:

0000: 16 03 01 00 4*d* 01 00 00 49 03 01 44 2*c* 2*d* 1*f* 67

0010: 6*c* *e*5 05 *a*5 88 12 6*b* 8*f* *a*8 *d*3 *e*5 9*e* *e*0 55 *e*0 *bd*

0020: 99 24 *dd* *dc* 72 36 8*c* *c*7 18 *f*5 69 00 00 22 00 39

0030: 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30

0040: 00 2*f* 00 05 00 04 00 13 00 0*d* 00 16 00 10 00 00

0080: 99 24 *dc* 3*c* 78 36 83 e7 18 *f*5 69 00 00 22 00 39

00*a*0: 00 99 00 37 00 36 *ff* 35 ca *ca* 00 32 *eb* 31 00 30

Figure 1: The part of the virus code packet

Spoofing virus is the use of a computer virus into the internal system, the system program to the enemy or falsified system to "inject" false information, resulting in its decision-making mistakes weapons, such as "Jiao order type" virus, the virus code is part of the packet was shown in Figure 2:

0050: 77 2*f* 00 05 0*c* 04 c0 13 00 0*e* 00 16 00 10 00 00

0010: 6*c* *e*5 05 *a*5 88 12 6*b* 8*f* *a*8 *d*3 *e*5 9*e* *e*0 55 *e*0 *bd*

0000: 16 03 01 00 4*d* 01 00 00 49 03 01 44 2*c* 2*d* 1*f* 88

00*a*0: 00 99 00 37 00 6*f* *ff* 35 ca *ca* 00 32 *eb* 31 00 30

0020: 99 24 6*d* *dc* 12 36 8*c* *c*7 18 *f*5 69 00 00 22 00 39

00*c*0: 99 24 *dc* 3*c* 78 36 83 e7 18 *f*5 69 00 02 22 00 39

0040: 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30

0030: 00 2*f* 00 05 00 04 00 13 00 0*d* 00 16 00 10 00 00

Figure 2: Spoofing virus part of the code

In the figure the number of LAN traffic dig package "00 Oa eb 63 17 40" is DA, but "00 0a eb 26 2d 32" is SA, "05dc" indicates the length of the packet is 1500 bytes, and other data DATA is content with the PAD.

3. Experiments and results

3.1 Computer communication network model and protocols

It must be considered when designing a LAN network speed, distance and cost required for the connection. The main factors affecting the LAN connection is a fair distance from the access mechanism. The two most common access mechanism is CSMA/CD and token passing, which are mapped to Ethernet and token ring. The agreement with the formation of the 10BASE-T Ethernet was shown in Figure 3:

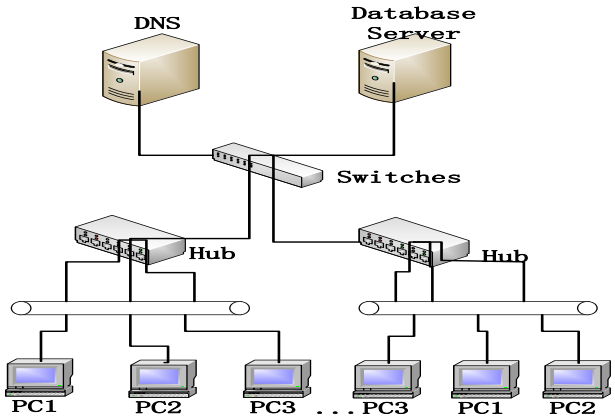

Figure 3: The agreement with the formation of the 10BASE-T Ethernet

10BASE-T unshielded twisted-pair is 10Mbit / s Ethernet transmission rate, its technical features is the use of an existing 802.3 media access control (MAC) layer, via a media attachment unit (MAu) and 10BASE-T physical media connected. T physical media uses two pairs of category 3 UTP, wire terminations that meet ISO standards Iu45 plug, line length up to 100m, the signal frequency range of 1020MHz, typical network equipment network cards, hubs, switches, and servers.

Ethernet networking is simple, fast, cost-effective, reliable transmission of information, traditional data transmission network application more excellent solutions, so it is used in a large number of theater between civil and / Army garrison command center and at all levels of the engine room communications.

3.2 Reliability optimization analysis

Cost matrix C_0 and computer network computer network link reliability matrix R_0, respectively, as shown below.

$$C_0 = \begin{bmatrix} 0 & 5 & 8 & 12 & 14 & 7 \\ 5 & 0 & 9 & 4 & 8 & 11 \\ 8 & 9 & 0 & 5 & 10 & 9 \\ 12 & 4 & 5 & 0 & 3 & 7 \\ 14 & 8 & 10 & 3 & 0 & 6 \\ 7 & 11 & 9 & 7 & 6 & 0 \end{bmatrix} \tag{9}$$

$$R_0 = \begin{bmatrix} 0 & 0.98 & 0.95 & 0.99 & 0.999 & 0.96 \\ 0.98 & 0 & 0.97 & 0.988 & 0.996 & 0.99 \\ 0.95 & 0.97 & 0 & 0.96 & 0.95 & 0.988 \\ 0.99 & 0.988 & 0.96 & 0 & 0.93 & 0.92 \\ 0.999 & 0.996 & 0.95 & 0.93 & 0 & 0.96 \\ 0.96 & 0.99 & 0.998 & 0.92 & 0.96 & 0 \end{bmatrix} \tag{10}$$

End conditional simulation genetic manipulation is the number of iterations is 100 times. Computer network link cost simulation graphs and computer network reliability simulation curve was shown in Figure 4, respectively.

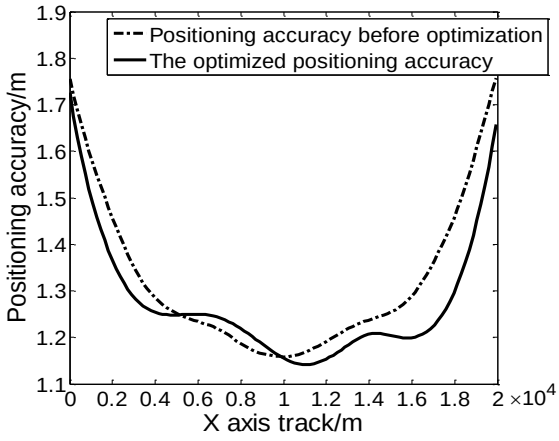

Figure 4: Computer network link cost simulation graphs and computer network reliability simulation curve

To ensure that computer networks can achieve maximum performance, you should master the rules of computer network failure occurs and its impact on the normal work produced, and to consider appropriate measures. Computer network optimization network design is a systematic project, to be considered at the meet business performance requirements, and to ensure the reliability of the premise, as far as possible to control costs; or in the provision of certain preconditions, a computer network can not only meet business requirements and to ensure the stability to maximize.

As can be seen from Figure 5, the anti-virus computer network attacks radiation safety is inversely proportional to the radius of the coupling length, the greater the coupling length, the smaller the safety distance, at the same time it can be seen, the coupling affects the length of the radius of network security is not radiation injected power significantly.

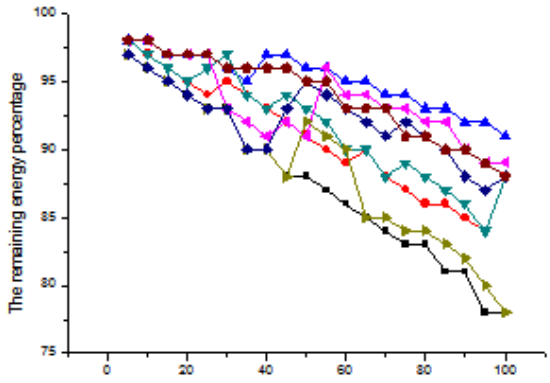

Figure 5: Security loom and half the coupling length simulation

As can be seen from the above simulation, safety and radiation protection radius injected power is proportional to the radiation computer network antivirus attack, the relationship is inversely proportional to the length of the cable coupling. Thus to achieve the radiation injected into the virus, which is normally radiated power must be large enough for the characteristics of the radio, using the 125W HF radio to meet in 50m virus injected radiation.

4. Conclusions

In this paper, the feasibility of computer networks against virus attacks are analyzed, pointing out the characteristics of computer virus weapon, injection methods and attacks, the last of a computer virus spread in the network to establish a relevant mathematical model, the simulation results, we can see a computer spread of the virus in the network speed and the number of infected machines varies with time, so as to implement computer virus attacks radiation information provided strong evidence. First proposed a computer model to attack the network and its communication protocol analysis, computer virus attacks radiation information

modeling, design and implementation of radiation virus attack scheme by analyzing the target data formats, encoding, modulation characteristics, the establishment of a virus attack information signal flow, to achieve the purpose of the network is to identify the enemy and run.

Reference

Arnason B.G., Jensen M.A., & White D.M., 2015, U.S. Patent No. 8,986,698. Washington, DC: U.S. Patent and Trademark Office.

Balog K., Azzopardi L., Rijke M., 2006, Formal models for expert finding in enterprise corpora. In: Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval, August 06-11, Seattle, Washington, USA, p 43–50. doi:10.1145/1148170.1148181

Balog K., Rijke M., 2007, Finding similar experts. In: Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval, Amsterdam, The Netherlands, p 23–27. doi:10.1145/1277741.1277926

Szekely G., Valtcheva I.B., Kim J.F. and Livingston A.G., 2014, Livingston, React. Funct. Polym, DOI:10.1016/j.reactfunctpolym.2014.03.008.

Kuzushima K., Ito Y., Okamura A., Akatsuka Y., & Morishima Y., 2013, U.S. Patent No. 8,481,051. Washington, DC: U.S. Patent and Trademark Office.

Li S., 2014, Potency of nanoparticles to amplify radiation effects revealed in radioresistant bacteria (Doctoral dissertation, Paris 11).

Programme U.N.E., 2016, Environmental effects of ozone depletion and its interactions with climate change: progress report, 2015. Photochemical & Photobiological Sciences, 15(2), 141-174.

Ramana C.V., & Kumar B.M., 2016, Virus Attack Identification And Representation In Sensor Network. IJSEAT, 4(1), 040-043.

Seager S., Schrenk, M., & Bains, W., 2012, An astrophysical view of Earth-based metabolic biosignature gases. Astrobiology, 12(1), 61-82.

Site, E., 2015, Massachusetts General Hospital| Imaging. US News & World Report, 11, 1.

Tang S., Myers D., & Yuan J., 2013, Modified SIS epidemic model for analysis of virus spread in wireless sensor networks. International Journal of Wireless and Mobile Computing, 6(2), 99-108.

Tu J., Inthavong K., & Ahmadi G., 2012, Computational fluid and particle dynamics in the human respiratory system. Springer Science & Business Media.