RCES REVIEW OF COMPUTER ENGINEERING STUDIES

ISSN: 2369-0755 (Print), 2369-0763 (Online)
Vol. 4, No. 1, March 2017, pp. 36-40
DOI: 10.18280/rces.040107

A publication of IIETA

IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering
http://www.iieta.org/Journals/RCES

Computer cyber security analysis as well as results

Soumen Chakraborty

Department of Information Technology, MCKV Institute of Engineering, MAKAUT, West Bengal, India

Email: csoumen88@gmail.com

ABSTRACT

This paper presents an introduction to a useful predicament of effects to our on-line world i.e. Cyber assaults and safety. In starting of the paper we describe the objects used for cyber assaults and inform the method of spreading them akin to secondary reminiscence, e mail attachments, instantaneous messages or malicious bots. After this paper describe the roll of mathematical modeling and simulation to unravel the predicament with an tremendous mathematical overview.An analysis of the most important variety has been made. We derive global steadiness of a worm-free state. Additionally, initial simulation outcome show off the optimistic influence of increasing security measures on worm propagation in various group.Efficiency of antivirus program and crashing of the nodes accordingly of worms attack is seriously analyzed.Numerical method is employed to get to the bottom of the procedure of equations developed and interpretation of the yields wonderful revelations Cyber safety structure and viable factors of cyber look after model are moreover studied for locating the research gaps. On the final this paper finds some gaps and possible tactics to bridge these gaps.

Keywords: Virus, Worms, Differential Equation, Illustration Messaging, FTP, E-Mail

1. INTRODUCTION

The arrival of internet/neighborhood science in prior three many years has resulted in sea exchange in the way in which data is transferred and understanding alternate takes function. By way of the years coupled with technological growth and need, internet technology has grown, offering countless functionalities and services. The growth of web science has thrown extreme challenges in kind of requirement of a suitable cyber safeguard approach to preserve the valuable understanding stored on approach. In the direction of this reason it can be proposed to be educated and totally seize the really numerous malicious objects and support a mathematical model to represent their habits [1], [2]. Originally, we did the be taught of self-replication and self-propagation of malicious objects identical to virus, worm, laptop virus, Bots and plenty of others. [1], [2]. Bodily Static mannequin: These physical models don't trade their habits as time adjustments like- water-tank model. Bodily Dynamic mannequin: These bodily units alternate their habits as time adjustments like spring suspension method or same electrical process.

Mathematical Static: These mathematical units provide a mathematical equation when the approach is in equilibrium state like- demand give strategy.Mathematical Dynamic mannequin: In these mathematical models permit the trade of approach attributes due to the fact the function of time like- oscillatory action.

Mathematical Static Analytical model: these are small static mathematical mannequin which will also be solved via typical math. Mathematical Static Numerical mannequin: These are tricky static mathematical model which will also be solved by way of simulation.

Mathematical Dynamic Analytical mannequin: these are small dynamic mathematical model which can also be solved through making use of common math.

2. REFINED INFLUENCE METHODS

The assaults on the desktop are absolutely stochastic. We do not comprehend the specific time of subsequent assault on the computer. Nevertheless, on the groundwork of risk principles in simulation we can in finding the likelihood of the assault at an instance of time. If stochastic variable (Time taken) can take exceptional values, xi (i = 1, 2, …, I), and the hazard of the value xi being taken is P(xi), the set of numbers P(xi) is claimed to be a risk mass perform. Due to the fact that the variable have obtained to taken one of the values, it follows that likelihood mass perform will even be outlined as P (xi) = ni / N

The position N= whole number of assaults and ni wide variety of assaults from a targeted source. A cumulative

distributed perform can also be observed which offers the possibility of stochastic assaults' being slash than or equal to a given price. Distinct measures of probability functions can also be utilized for the achieve potential of of the stochastic method similar to indicate, mode, median, typical deviation, and many others. Items attribute equations can be of two types – Linear and non-Linear. Non-linear process will even be represented by way of Partial Differential Equations (PDE). Don't forget that malicious object has propagation property P, is determined by quite a lot of unique explanations like- A, B, C …and so on. It can be represented as

P=f (A, B, C...).

The speed can be represented as

$\partial P/\partial t = \partial f (A, B, C,...)/\partial t$.

And the acceleration expense may even be represented as

$\partial^2 P/\partial t^2 = \partial^2$

f(A,B,C,…)/ ∂^2

as quickly as the simulated results bought by the use of special approximation techniques stated beneath can be utilized for complementing the information generated through utilizing simulation as good as

3. VALIDATION RESULTS FOR EVALUATION

The sequence expansion: Any function that has derivatives may also be extended by way of Taylor's formula, the worth of the impartial variable, x, in a neighborhood close x = a, a perform f(x) will also be approximated via the polynomial

F(x) = f(a) + f'(a)(x-a) + (f''(a)/2!)*(x-a)2 +…..+

(f(n)(a)/a!)*(x-a)n

4. FINITE ALTERNATE APPROXIMATION METHODS

This method transforms a partial deferential equation over small intervals.

That is of two types-ahead change Approximation: It calculates the perform gradient at various factors by way of the formulation:

f'(xi) = (f(xi+1) – f(xi))/ Δx

Backward difference approximation: It moreover calculates the perform gradient at quite a lot of features via utilising the procedure:

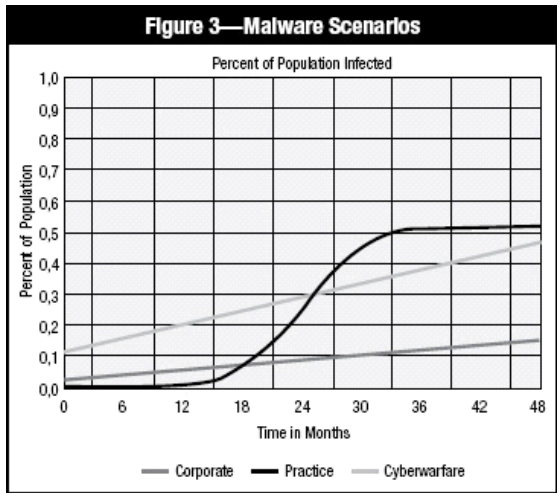
f'(xi) = (f(xi) – f(xi-1))/ Δx

Higher order derivatives: These may also be calculated to describe the various major elements in the distribution with the aid of using the next formula

(n) = (f(n-1))

Some regression assessments similar to Polynomial regression checks will also be used to validate the model. It finds that the values may also be equipped proper into a polynomial or now not. As soon as the attribute equation is derived then outcome can be empirically/analytically validated on the groundwork of on hand ordinary mathematical speculation. The very first thing for mathematical mannequin validation is the dimensional homogeneity, which requires that each and every term has the equal web dimensions [3].

Secondly, the models may also be validated by means of checking qualitative and limit habits. Apart from these some distinct issues may also be viewed, depending on how significant the errors are? What's the accuracy and precision? Are the abilities equipped into the uniform curve? The data may also be prepared by utilizing imply, mode, median or common deviation. This expertise can be when compared with no hindrance and support us to recognize the conduct of malicious objects [4].



5. QUANTITATIVE ANALYSIS AND MATHEMATICAL OUTCOME

We assume that the total populace within the neighborhood at any instance t is

N(t) = S(t) + I(t) + R(t).

Virus and worms is assumed to be in the computing device community for a minimum of a time θ = max(ω, τ), so that the preliminary perturbation have ceased. The techniques of equations for the result as per our assumptions take the following varieties for t > θ:

dSk(t)dt = mk(bN(t)) + (γkIk(t − τ)e −μτ) − μSk(t)−λkSk(t)dIl(t)

dt = αβc I(t − τ)

N(t − τ)

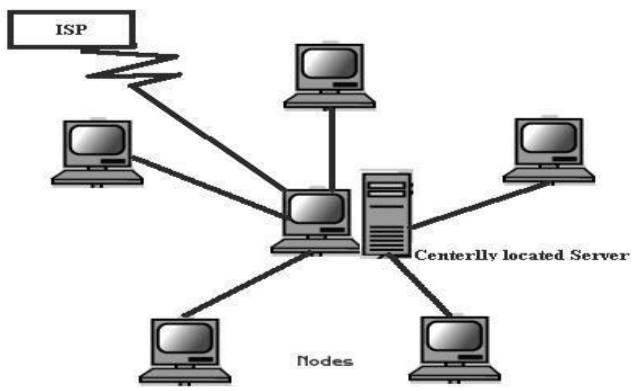
S(t − τ).E−μτ+[pkαβc I(t − (τ + ω + φk))

N(t − (τ + ω + φk)).S(t − (τ+ω + φk)).Rk.E−μ(ω+φk)]dRk(t)

dt =Xn

j=1

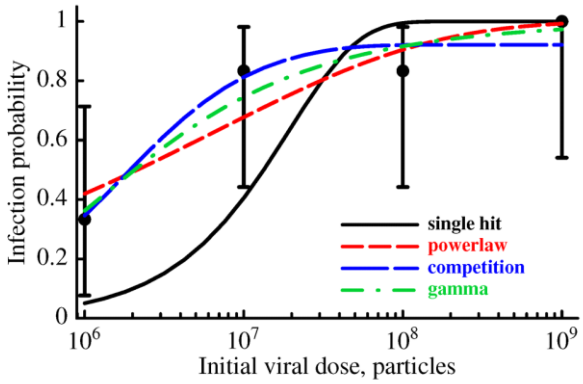
[qkγkIk(t) − γkIk(t − τ)e−μτ − εkR(t)]−μR(t) (5)



6. PROBABILISTIC SEIRS VARIATIONS RESULTS

In the time prolong mannequin, parameter, γ, represents the chance of spreading the infection in a single contact. It's apparent that the cost of propagation is proportional to the connectivity of the node. The propagation price does now not alternate in time for the period of the group. With a rationale to capture additional realistic dynamics inside of actual world

scale free networks, a couple of extra variables in evaluation with the classical SIR mannequin are used and to capture further realistic habits, lengthen is don't forget on the neighborhood. An additional stage (uncovered) within the mannequin represents the phenomenon of incubation, most important to a lengthen between susceptibility to contamination and special infection. The uncovered stage makes the mannequin a SEIR mannequin as a substitute of a SIR model. Additionally, the pSEIRS mannequin is one-of-a-sort from the classical SEIRS mannequin (the latter is purchased for an immunity likelihood p = 1). The ensuing mannequin is described in phrases of the subsequent.



7. VARIABLES AND CONSTANTS FOR BEST RESULTS

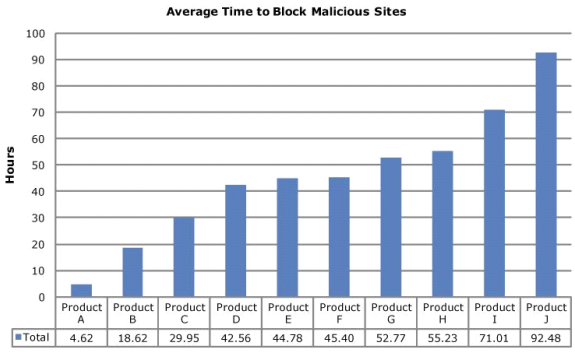
N (t): complete populace dimension
S (t): prone populace
E (t): uncovered populace
I (t): contaminated population
R (t): Recovered populace
β: beginning expense.
μ: dying cost as a result of motives as a substitute than an illness with the help of an epidemic.
ε: demise price due an illness through a virulent sickness, it can be constant.
α: healing cost which is general.
γ: typical quantity of contacts of a node, moreover equal to the threat of spreading the virus in
one contact.
ω: Latency interval or time lengthen, which is a consistent i.E., the time between the exposed.
7. Methods of experimental results:
τ: interval of transitority immunity, which is a constructive typical.
P: chance of temporary immunity of a node after recuperation.

As soon as an contamination is presented into a group, its nodes will become inclined to the sickness and, in due direction, will get infected. Once a node is uncovered, an incubation interval is discovered, which is captured through the new time extend parameter, which for that reason items reality bigger: any sickness goes through an incubation interval prior than it propagates. After illness, anti-virus software may be implemented to treat an contaminated node, consequently, delivering it with temporary immunity. It is principal to realise that there's no permanent immunity in an actual group, thus an immune node may just revert to the inclined stage once more. All these levels of health problem from inclined to Recovered, and the phases in between. The assaults on the computer are utterly stochastic. We have no notion the actual time of subsequent assault on the laptop. However, on the foundation of danger concepts in
simulation we will in finding the probability of the assault at an illustration of time. If stochastic variable (Time of assault) can take I uncommon values, xi (i = 1, 2, …, I), and the likelihood of the worth xi being taken is P(xi), the set of numbers P(xi) is purported to be a probability mass perform. On account that the variable ought to taken probably the most values,
it follows that
$I\Sigma\ P\ (Xi\ ) = 1$
i=1
likelihood mass perform can even be outlined as
P (xi) = ni / N
where N= complete number of assaults and ni number of assaults from a distinct supply.

A cumulative allotted operate can be placed which presents the possibility of stochastic assaults' being lower than or equal to a given cost. Nice measures of probability capabilities can be used for the study of the stochastic system reminiscent of imply, mode, median, typical deviation, etc.
Objects attribute equations can also be of two types – Linear and non-Linear. Non-linear system will even be represented through Partial Differential Equations (PDE). Recall that malicious object has propagation property P, is determined by more than a few different factors like- A, B, C …and many others. It can be represented as
P=f (A, B, C...).
The % can also be represented as
$\partial P/\partial t = \partial f\ (A, B, C)/\partial t$. And the acceleration rate will also be represented as

$\partial^2 P/\partial t^2 = \partial^2 f\ (A, B, C)/\partial t^2$.

As soon as the simulated effect bought via certain approximation procedures recounted below can be used for complementing the information generated through simulation as just right as validation: -
Taylor sequence progress: Any operate that has derivatives may also be improved with the help of Taylor's system, the valued at of the impartial variable, x, in a neighborhood close x = a, a operate f(x) will also be approximated via utilising the polynomial
F(x) = f(a) + f'(a)(x-a) + (f''(a)/2!) *(x-a)2 +…..+ (f(n)(a)/a!)*(x-a)n.



Finite trade approximation tactics:

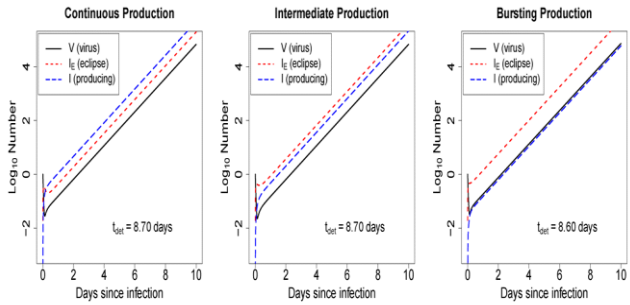
This process transforms a partial deferential equation over small intervals. That is of two types ahead change approximation: It calculates the operate gradient at more than a few facets with
the aid of the method:
f'(xi) = (f(xi+1) – f(xi))/ Δx

Backward change approximation: It additionally calculates the perform gradient at more than a few facets by way of the formulation:
f’(xi) = (f(xi) – f(xi-1))/ Δx
larger order derivatives: These can also be calculated to describe the more than a few main sides within the distribution via the following add-onsf(n) = (f(n-1))’
Some regression exams comparable to Polynomial regression checks may also be used to validate the mannequin. It finds that the values.For a category of populace, e-SIRS mannequin with normal latent interval(!), immunity period(¿) and replication interval(Áok) is developed maintain-ing in view the replication advice of malicious buyers. Whenever a node is infected there may be danger of malware getting replicated with replication aspect rk. After a node has been integrated within the infective classification, it'll self-replicate with a chance pk and will not self-replicate with a possibility (1 ¡ pk). In our mannequin when a node is eliminated from contaminated class it recovers briefly and acquires temporary immunity with probability qk or the node may just vanish with likelihood (1 ¡ qk) [33] regarded the restoration from contaminated classification acquiring permanent immunity with probability q. The recovered node stays in state of temporary immunity for a time interval of previous than it becomes inclined once more. The long-term work will handle on the endemic equilibrium and its steadiness & ailment-precipitated mortality.

Translation of NFA Identification into an INLP the mission of NFA induction shall be formulated, then it is going to be re-formulated as an INLP. Let Σ be an alphabet, let S+ (examples) and S− (counter-examples) be two finite sets of phrases over Σ, and let ok be an integer. The goal of NFA induction is to investigate a k-state NFA A = (Q, Σ, δ, s, F), as outlined in Hopcroft et al. (2001), such that L(A) includes S+ and is disjoint with S−.
Let S = S+ ∪ S− (S+ ∩ S− = ∅), and let P(S) be the set of all prefixes besides for the empty phrase of all phrases of S. The integer variables perhaps xpq * zero, 1, p * P(S), q * Q;yaqr zero, 1, a * Σ, q, r * Q; and zq * zero, 1, q * Q. The valued at of xpq is 1 if q * δ (s, p) holds in
an automaton A, xpq = zero otherwise. The value of yaqr is 1 if r * δ (q, a), yaqr = zero
otherwise. Eventually, we let zq = 1 if q ∈ F and 0 if no longer. Let us now see how to describe the constraints of the connection between an automaton A and a suite S in terms of nonlinear equations and inequalities.
1. Naturally, regular with the presence of the empty phrase we require that
zs = 1 λ * S+
zs = 0 λ ∈ S−

$$\begin{aligned}
\Pr(X_i(t+\Delta t)=0 \mid X_i(t)=0) &= 1-\left[\beta_1\sum_j a_{ij}I_j(t)+\beta_2\sum_j a_{ij}b_j(t)\right]\Delta t+o(\Delta t),\\
\Pr(X_i(t+\Delta t)=1 \mid X_i(t)=0) &= \left[\beta_1\sum_j a_{ij}I_j(t)+\beta_2\sum_j a_{ij}b_j(t)\right]\Delta t+o(\Delta t),\\
\Pr(X_i(t+\Delta t)=2 \mid X_i(t)=0) &= o(\Delta t),\\
\Pr(X_i(t+\Delta t)=0 \mid X_i(t)=1) &= \gamma_1\Delta t+o(\Delta t),\\
\Pr(X_i(t+\Delta t)=1 \mid X_i(t)=1) &= 1-\gamma_1\Delta t-\alpha\Delta t+o(\Delta t),\\
\Pr(X_i(t+\Delta t)=2 \mid X_i(t)=1) &= \alpha\Delta t+o(\Delta t),\\
\Pr(X_i(t+\Delta t)=0 \mid X_i(t)=2) &= \gamma_2\Delta t+o(\Delta t),\\
\Pr(X_i(t+\Delta t)=1 \mid X_i(t)=2) &= o(\Delta t),\\
\Pr(X_i(t+\Delta t)=2 \mid X_i(t)=2) &= 1-\gamma_2\Delta t+o(\Delta t).
\end{aligned}$$

2.Traditionally the most above equations are required provided that λ * S. Within the opposite case, the variable will need to no longer be settled in advance. Every illustration desires to be authorized by means of the automaton, however no counter-illustration need to be. This can also be written as
XqQ
xpqzq ≥ 1 p ∈ S+ − λ
XqQ
xpqzq = zero p ∈ S− − λ
3. For P(S) three p = a * Σ we're able to have xpq equal to 1 best in occasions in which q * δ(s,a);
accordingly, xpq − ypsq = zero p ∈ a ∈ Σ, q ∈ Q
4. In the end, we have to exact the fact that every time xpq = 1 for p = wa, w Σ+,
a * Σ, now we've q * δ (r, a) for a minimum of one state r such that xwr = 1. And vice versa,if a phrase w is spelled out by using utilizing a route from s to a state r and there is a transition ra −→ q, then xpq = 1 needs to be fulfilled. We're in a position to guarantee this by means of requiring
−xpq +XrQ
xwryarq ≥ zero p ∈ w ∈ Σ+ ∧ a ∈ Σ
xpq − xwryarq ≥ 0 q, r ∈ Q



Reasoning regarding the right finish is an identical.

Let t, be the first time step t prior than the error interval J’ with the property that for some i now we have t <s;, l(t) > 3iw3. Let t, be the main time-step after J’ with the equal property. We are able to expect without lack of generality that each t, and t, exist:
1. If l(s,+,)< 3iw3 for some i then there isn't any tj after s~+~. Definitely, the approach reduce(i+ 1) does not prolong the gaps in [0 ... 3(i+ 1)~~). If there is no tj before s1 then l(s,) = 0 and the condition is fulfilled. Suppose therefore tl < s1 .
2. Suppose that tj is in [0 . . S, - 4.5w3d,] for some j. Via Lemma 13.2 if the left endgap persevered except tj+ 2.5w3d, then it might now not ever be healed. By the point s,it could be extended to a dimension of at the least 3w3, besides the fact that children that the error decreases it maximally. After that, cut back (1) would prolong it over the entire block. Considering this does no longer happen, we have I(tJ) = zero for some t; < tj + 2.5w3d, and l(t) < 2.5~~ for all t
in [tie.* $1.
3. If the assumption 2 holds for j= 1, 2 then it follows from 1 that the statement of the lemma is proved. Suppose therefore that the assumption 2 does not hold for j= 1. Then we have l(t) < SW’ for all t in [s, + c1 *.*.S,].We will be able to be able to show that there is a t; in [s, . . . S1 +2.5w3d,] such that l(t;) d 3w3, and Z(t)<6w3 for all tin [s,*..T;].If I(s,) < 3w, then we can choose t; = si. If l(s,) > 3w3 then through Lemma thirteen.2, if the situation l(t) > 3w3 persists unless s1 + 2.5w3d, then it's going to absolutely no longer be repaired and it kills the block. As a outcome we can have Z(t;) < 3w3 for some t’, < s1 + 2.5w3d, and l(t) < 6w3 for all t in [si ... T].
4. If t, < ti then condition 1 is fulfilled for i = 1. If t, > t; then the extension of the left endgap is error-free after t,, and is not

going to kill the block provided that now we have obtained l(t) <6w3 for all t in [t2-.S2].
5. If the belief 2 holds for j= 1 but does now not keep for j = 2 then the argument in four will also be repeated yet again, now with the t; outlined in 2.

8. QUANTITATIVE RESULTS AND DISCUSSION

An intuitionistic fuzzy record L on a suite X is characterized by using utilizing its perform operate
PL outlined as: ( ) LP X J P N × →
the situation J = X ≤ ≤ (α ,β) : α,β [0 ,1 and 0] α + β 1 and P(N) is the set of all subsets of N.
For this reason, for any x * X and (α,β) J, PL(x, (α,β)) grants the set of positions wherein the detail x happens in L with grade of membership (α,β).
An intuitionistic fuzzy file is an extension of a fuzzy file. The intuitionistic fuzzy expertise constructions like intuitionistic fuzzy STACK (IF-STACK), intuitionistic fuzzy QUEUE (IFQUEUE) and intuitionistic fuzzy ARRAY (IF-ARRAY) are the extension of their corresponding fuzzy models.Quite a lot of operations on STACK/F-STACK, QUEUE/F-QUEUE and ARRAY/F-ARRAY will also be elevated to stipulate them on IF-STACK, IF-QUEUE and IFARRAY in a average approach. So, we leave out them.

9. CONCLUSION

By way of inspecting the traits of pc viruses carefully, the disorders of some prior epidemic units of viruses had been indicated. On this groundwork, a common epidemic model of viruses the SLBS mannequin has been situated, and a few of its generalizations had been entreated.Toward this direction, a great sort of special models with parameter restrictions are yet to be investigated. Besides, the normal SLBS model is headquartered on completely connected networks and consequently can't seize the outcomes of the topological structure of the web on the spread of computer viruses. It will be particularly profitable to be trained the qualitative residences of the SLBS model on scale-free networks. Virus and worms in every employee have homogeneous susceptibility however susceptibility of virus and worms from exact staff is specific. Virus and worms in every infected staff (as per their susceptible conduct employees) has homogeneous health problem nevertheless infection of malicious objects from specified personnel is unique.For the case the location the number of contacts is proportional to the whole population

ACKNOWLEDGMENTS

It is a great honour for the all editors,reviewers and authors who have supported there effort in the research and development of this area of topics,also there motivational support for further future development and advancement in the field of computer virus as well as security of computer in day to day life.

REFERENCES:

[1] Saini D.K. (2011). A mathematical model for the effect of malicious object on computer network immune system, *Applied Mathematical Modeling*, Vol. 35, pp. 3777-3787, DOI: 10.1016/.2011.02.025

[2] Mishra B.K., Saini D.K. (2007). Mathematical models on computer viruses, *Elsevier International Journal of Applied Mathematics and Computation*, Vol. 187, No. 2, pp. 929-936.

[3] Saini D.K., Saini H. (2008). VAIN: a stochastic model for dynamics of malicious objects, *the ICFAI Journal of Systems Management*, Vol. 6, No. 1, pp. 14- 28.

[4] Saini H., Saini D.K. (2007). Malicious object dynamics in the presence of Anti Malicious Software, *European Journal of Scientific Research*, Vol. 18, No. 3, pp. 491-499.

[5] Fixed Coefficients Block Backward Differentiation Formulas for the Numerical Solution of Stiff Ordinary Differe ntial Equations Ibrahim. pp. 508-520. ISSN 1450-216X.

[6] Chen T., Jamil N. (2006). Effectiveness of quarantine in worm epidemics, *IEEE International Conference on Communications*, pp. 2142-2147.

[7] Keeling M.J., Eames K.T.D. (2005). Network and epidemic models, *J. Roy. Soc. Interf.*, Vol. 2, No. 4, pp. 295 – 307.

[8] An epidemiological model of virus spread and Cleanup, Matthew M. Williamson,HP Labs Bristol,

[9] Filton Road, Stoke Gifford, BS34 8QZ, UK Newman M.E.J., Forrest S., Balthrop J. (2002). Email networks and the spread of computer virus, *Phys. Rev. E,* Vol. 66, pp. 035101-1-035101-4.

[10] Draief M., Ganesh A., Massouili L. (2008). Thresholds for virus spread on network, *Ann. Appl. Prob*., Vol. 18, No.2, pp. 359 – 369.

[11] Li G., Zhen J. (2004). Global stability of an SEI epidemic model with general contact rate, *Chaos Solitons and Fractals*, Vol. 23, pp. 997–1004.

[12] Stability theory for ordinary differential equations, J.P LaSalle. Author links open the author workspace. Center for Dynamical Systems, Brown University.

[13] Krieger, Basel, (1980) 12] J. O. Kephart, A. (1995). Biologically inspired immune system for computers, *Proceedings of International Joint Conference on Artificial Intelligence*, pp. 137-145.

[14] Kephart J.O., White S.R. (1993). Measuring, and modeling computer virus prevalence, *IEEE Computer Security Symposium on Research in Security*, *and Privacy*, pp. 2-15.

[15] Kephart J.O., White S.R., Chess D.M. (1993). Computers, and epidemiology, *IEEE Spectrum*, Vol. 30, No. 5, pp. 20-26.

[16] Kermack W.O., McKendrick A.G. (1927). Contributions of mathematical theory to epidemics, *I, Proceedings of the Royal Society of London, Series A*, Vol. 115, pp. 700-721.