J. Basic. Appl. Sci. Res., 2(11)11542-11550, 2012
© 2012, TextRoad Publication
ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A New Method for Proactive Worm Propagation Modeling in Peer-to-Peer Networks

Mehdi Gorbanloo[1], Mohammad Abdollahi Azgomi[2]

[1]Computer engineering department , Azad university , Zanjan , Iran
[2]Computer engineering department , Science and Technology University , Tehran , Iran

ABSTRACT

Proactive worms will be the most serious threat to internet infrastructures in the near future . their latent threats have made researchers to work on modeling and analysis of propagation of proactive worms . In this paper two important model of worms propagation in a unstructured network has been studied and limitation and drawbacks of them are explained then a novel method called "MPropagation" with simulation and experimental results to solve their problems is presented .It will be indicated that this method is more accurate and close to real and not has previous problems which is lack of dynamics and not considering operative and substantial parameters of worms propagation such as bandwidth and infected file size .This method also has dynamic property . validation of this model proper working is presented by simulating with Peersim simulator software .

KEYWORDS: worms propagation, network topology, configuration variety, four-factor model, peer-to-peer networks.

INTRODUCTION

A peer to peer (P2P) worm is a harmful code that can be spread from one machine to another using P2P network [1]. P2P networks are turned into worms propagation carrier because of their three inherent specifications . First, the hackers is attracted due to great number of P2P homogeneous clients since users are forced to perform their program in the terminal to achieve their services . Second, P2P topology increases the effluence rate of the worms because they search influent aims to achieve by Neighbors information . Third, recognition of P2P worms is difficult owing to their affection on normal traffic [2] . Unstructured P2P networks are distributed systems in the nature such that they have no hierarchy organization or centralized control [3]. The worms classify into three categories : Passive, active and proactive , each in different propagation model . Remainder of article is classified as follows :At first section relayed works about worms propagation in unstructured P2P networks are presented .Second section investigates present models and depicts drawbacks of them and then represent proposed model MPropagation with some advantages to solve their problems .This method advantages can be divided into : 1) accuracy 2) bandwidth spotting 3) infected file size containing 4) dynamism 5) proximity to real environment . This paper Only deals with unstructured P2P network issues using software simulation . In section three simulation results which are performed by Peersim and matlab simulation software ,are illustrated diagrammatically and statistically . section four contains conclusion .This article tries to show unstructured P2P networks drawbacks and endeavors to present new approach to overtop those problems using reliable simulation results.

1. Related works

1.1 Traditional models

Traditional models were primary models without considering the network topology . However , major part of the new models in P2P network are based on this traditional models . In the simple epidemic model (SEM) , each host is in one of two following states: Susceptible or infected . The state of each host is such that can transfer from susceptible to infected case so that in a finite network all are infected at the end . while in Susceptible-infected-Susceptible (SIS) each susceptible node can be infected . and each infected group can be recovered and again be susceptible to infection . every host node in SIS model executes (susceptible-infected-susceptible) cycle repeatedly . Susceptible-Infected-Removed (SIR) model removes the infected hosts processing . Each of the hosts in SIR model can be recovered or removed . When a host is got cleaned of infected host state it is immune to different kinds of worms and is remained at removed (cleaned) state forever . Each of the hosts in SIR model is in transition state (removed-infected-susceptible) or is in susceptible state . Two –factor model is an improved SIR model . it proves that Human countermeasures and congestion of routers can reduce the worms propagation rate . each host is in two –factor or in transition (removed, infected, susceptible) or in (removed-susceptible) state that finally in a susceptible network all hosts are removed(cleaned) [2] .

***Corresponding Author:** Mehdi Gorbanloo, Computer Engineering Department, Azad University, Zanjan, Iran

1.2 Evolutionary models in P2P networks

Most of the propagation models of P2P proactive worms are derived of the traditional models , which explained previously. Some researchers have linked SEM model with P2P networks . They comprehend that P2P topology increased the propagation rate of the proactive worms . When the worms get efficient in searching for the goals by the neighbors information, raise a model, improved of SIS model . This Follows two results : First, suppressing P2P proactive worms is difficult due to their high propagation rate , second , worms propagation rate in the case of objective selection from a node with more connection degree is faster than a node with less connection degree . Lidong Zhou et al. (2005) presented some concepts of P2P worms and their threats . They used BA-based model in their study and considered a high limit of infected peers in their defense infrastructures in a theoretical analysis but they didn't use P2P worms' propagation model [4] . Jayanth Kumar Kannan et al. Designed a worm used to implementation different kinds of political goals to bypassing the controlled existing worm propagation and their simulations plans . Result again demonstrated that a P2P worm can be developed more than other worms. Like Weiyu Slammer mathematics based general models for the worms for defenders/ attackers using some models of various systems [5]. They proved that the number of new infected peers and average number of neighbors have exponential enhancement but difference between logical topologies was not considered . Jie Ma et al. defined passive P2P worm propagation model analyzing some effects of P2P factors using numerical analysis . They didn't focus on P2P proactive worm [6] . Zhany et al. modeled P2P network as a graph . they used discrete time to do Recursive analysis and performed absolute approximation to describe Recursive analysis and absolute approximation to describe the propagation of proactive P2P worms and performed extensive simulation studies [7] . Jiaq and Binxiao et al. designed noved worm named by DHL . BT networks can find new victim and propagates itself by requesting a router to make a dynamic hit list and reviewing the affects of each worm parameters [8] . The worm they made was only suitable for BT and suchlike networks .

2. Worms propagation models

2.1 Two-factor model

Two-factor model was proposed in [9],[10] as expressed above . This model shows clearly that two-factor have more effect on worms' propagation . of these factors one can point to dynamic Human countermeasures such as cleaning, assembly and filtering . these Human countermeasures can transfer some information about the hosts at susceptible and infected state to removed (cleaned) one . R(t) represents number of removed hosts of infected ones. R(t) instantaneously rate is :

$$\frac{dR(t)}{dt} = \gamma I(t) \quad (1)$$

Where I(t) indicates number of infected hosts , γ is a constant illustrates removing rate of infected hosts . Q(t) expresses removed hosts of susceptible ones . Q(t) instantaneously rate is :

$$\frac{dQ(t)}{dt} = \mu S(t) J(t) \quad (2)$$

Where S(t) is the number of susceptible hosts . μ is a constant illustrates removing rate of susceptible hosts . J(t) indicates number of infected hosts which is expressed as :

$$J(t) = R(t) + I(t) \quad (3)$$

Reduction of infection rate of two-factor model is :

$$\beta(t) = \beta_0 \left[1 - I(t)/N\right]^{\eta} \quad (4)$$

Where β_0 is the initial value of infection rate . η is used to regulate infection rate sensitivity toward infected hosts (I(t)) . $\eta = 0$ illustrates constant quantity of infection rate . N depicts total number of investigated hosts .

The second factor is congestion and internet routers problem decreasing infection rate (β(t)) . Internet worms usually search their objectives by scanning a great number of IP addresses that are not observed by routers at normal conditions . Thus, when the internet got filled by worms, major number of abnormal scanning of packs can cause router congestion or rebooting it then reduction worms propagation rate . Two-factor model reduces infection rate [10] . Figure 1 depicts the conceptual diagram of two-factor model .

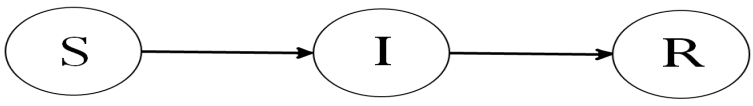

Figure 1: two-factor performing diagram

2.2 Four-factor model

Four-factor model is essentially derived of Two-factor model . It is developed version of Two-factor model which is expressed by Zhang et.al in 2009 . They asserted that there are four factors in terms of propagation properties of proactive worms in P2P unstructured networks that the previous models have not considered them completely.

1. Human countermeasures which result in removing both susceptible and infected hosts, as supposed in the classical two-factor model. the following actions can be taken to block worm propagation When any user is aware of proactive P2P worms: cleaning compromised computers, patching or upgrading susceptible computers , setting up filters to block the worm traffic on firewalls or edge routers, or even disconnecting their computers from the Internet [11].

2. P2P topology accelerates the propagation of proactive worms [7],[9],[12]. Instead of randomly searching for victims, proactive P2P worms acquire the targets from the cached neighbors' information [13],[7] .

3. Configuration diversity [14],[15] is capable of affecting worm propagation, but it is rarely considered in former models. Configuration diversity of each host in P2P networks can greatly decrease the overall vulnerability Hosts with largely different configuration diversities are unlikely to be infected by the same worm [15]. Configurations mentioned here include the operating system used, its version and patch level, additional software packages and executing applications with associated versions and open ports [15], [16].

4. Attack and defense strategies can also impact the propagation of proactive P2P worms. Here it is agreed with Feng *et al*. (2008) [9] that worms propagate faster when starting from the most connected node than from a random or the least connected node. As similar conclusion to [17] ,worm propagation can be reduced by immunizing some of the most connected hosts prior to worm propagation. In this paper, we have presented two strategies: random and target. Random denotes that the process of selecting nodes is random while target denotes selecting the most connected nodes. We do not take the routers' congestion into consideration since proactive P2P worms do not need to probe targets by blind scanning like Code Red worm [18],[19] and do not generate great traffic to flood routers [13]. Some other worms propagation models are presented in [20],[21],[9].

According to mentioned assumptions , Four-factor equations comes below [10] :

$$I(t+1)-I(t)=S(t)\times(1-\gamma)\times\left[1-\left(1-\frac{1}{N}\right)^{\Sigma di}\right]-\left[R(t+1)-R(t)\right] \quad (5)$$

$$S(t+1)-S(t)=-S(t)\times(1-\gamma)\times\left[1-\left(1-\frac{1}{N}\right)^{\Sigma di}\right]-\left[Q(t+1)-Q(t)\right] \quad (6)$$

$$R(t+1)-R(t)=\gamma I(t) \quad (7)$$

$$Q(t+1)-Q(t)=\mu S(t)J(t) \quad (8)$$

$$J(t)=I(t)+R(t) \quad (9)$$

Definition of parameters used in this model is listed in Table I .

Table I : some of parameters used in this model

N(t)	Total number of peers in p2p network as a function of time
S(t)	The number of susceptible peers in time t.
I(t)	The number of infected peers in time t.
R(t)	The number of secured or retrieved peers from infection in time t.
Q(T)	The number of retrieved peers susceptible state in time t.
J(t)	The number of infected peers or removed ones in time t.
γ	Cleaning rate of infected peers
μ	Cleaning rate of susceptible peers
V(t)	Set of infected peers which are changed from susceptible to infected state on period (t t+1)

2.3 MPropagation

At previous sections important present models have been discussed .Precise investigation of their equations resulted in that modeling using this method is completely peer- oriented .on the other hand , condition of peers is the only thing considered in propagation process . while , in worms propagation it is cleared that files contained worms have the most affect . The other point is that as infected file's size gets smaller , the propagation process gets faster . this is not considered in these methods . thus four- factor problems are classified as follows :

Not considering the number of files (infected and uninfected)
Not considering size of files (infected and uninfected)
Not considering band width for peers
Not considering download probability of infected files

Considering above problems , assumptions of proposed model are expressed. then model is explained based on them .

2.3.1 MPropagation model assumptions

The assumptions of the proposed model are as following . it is worth noting that some of the assumptions are presented due to simplification .

Assume that a host is infected and it attempts to infect all the neighbors immediately.

The numbers of online peers are dynamic. In this case infected or non-infected peers can enter to the network in simulation process .

The numbers of files are dynamic. In this case infected or non-infected file can enter to the network in simulation process .

searching , connecting , downloading and performing a file period is a fixed time called time units . A time unit is a range of time spends since a uploaded pair be damaged or stay protected .

When a pair infects , sends numbers of infected files to the neighbors represented in a value of "c".

Band width varies in the network .

The network communication is complete .it means for N peers, there are $\frac{N(N-1)}{2}$ links .

Susceptible peers can change from current state to Retrieved state directly such that it is shown in Fig.2 .

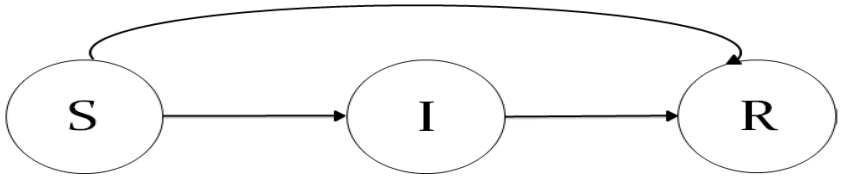

Figure 2 : state changing of peers in proposed model

To analyze proactive worms modeling , we raise the important parameters in propagation modeling .

2.3.2 MPropagation parameters

We assume that each host is added recently to the infected population tries to attack all the neighbors immediately . they will stay at the same state If new objective is infected or removed . Otherwise they will be infected in probability quantity of "$1-\delta$" if the goals are susceptible in the population . Thus, greater adjustments lead into less infection . $\delta = 0$ means that each susceptible host has been infected and $\delta = 1$ means that no susceptible host will be infected . It is proved that the change of the number of infected hosts from t to t+1 is :

$$S(t)(1-\delta)\left[1-\left(1-\frac{1}{N}\right)\right]^{\sum_{i\in V(t)} d_i} \qquad (10)$$

In a P2P network with infected files, the infected files can be downloaded when a susceptible peer downloads a file . Thus, possibility of downloading infected files is proportion with the ratio of infected files in the network . The total number of files in the network is *M(t)+K(t)* . Thus, possibility of downloading infected file is h (t) = $\alpha \frac{K(t)}{M(t)+K(t)}$ [22] . α is a Fixed corrector parameter . Fixed ratio α shows that probability of worm propagation is further . In a unit time , quantity of downloaded files by susceptible peer is λ_d and the probability of infection of files is h(t) . As it is known , downloading infected files rate depends on bandwidth of network and average size of infected files . it means whatever file size is smaller and band width is more , file download rate increases and vice versa . this phrase can be translated as an equation like this :

$$\lambda_{di} = \frac{BW}{S_i} \qquad (11)$$

Where BW is average band width of each peer and S_i is average infected files size . so, rate of S and I will vary . Because infection rate of peers depends upon download rate of infected files and downloading probability of infected files . Thus probability of infection of susceptible file on a unit time is $\lambda_{di} * h(t)$. It is clear that rate variation of I is opposite to S since by increasing the number of infected peers, the number of susceptible peers reduces . Thus, the probability of susceptible peer infection is $\lambda_d * h(t)$, then the rate of S changing is $-\lambda_{di} * h(t) * S(t)$. negative sign in S variation rate shows opposition of I and S rating change . When a susceptible peer be infected , the number of infected files is increased to " c ", the rate changing of k is

$\lambda_{di} * h(t) * S(t) * c$. Assuming that susceptible and infected peers are removed with the ratio $\lambda_{sr}\ S(t)$. $\lambda_{ir} I(t)$ respectively , change rate of removed peers is $\lambda_{sr}\ S(t) + \lambda_{ir}\ I(t)$. At the same time reduction rate of infected files is $c * \lambda_{ir}\ I(t)$. Thus, the equations in this model are as follow :

$$\frac{dS(t)}{dt} = -\lambda_{di} h(t) S(t) - \lambda_{sr} S(t) \qquad (12)$$

$$\frac{dI(t)}{dt} = \lambda_{di} h(t) S(t) - \lambda_{sr} I(t) \qquad (13)$$

$$\frac{dR(t)}{dt} = \lambda_{sr} S(t) - \lambda_{ir} I(t) \qquad (14)$$

$$\frac{dK(t)}{dt} = \lambda_{di} h(t) S(t) c - c\lambda_{ir} I(t) \qquad (15)$$

$$\frac{dM(t)}{dt} = \lambda_{dui} N (1 - h(t)) \qquad (16)$$

As newly infected hosts try to attack their neighbors immediately , there are $\sum_{i \in V(t)} d_i$ attacks in P2P network at time t . The probability to attack and the probability of no attack is 1/N and 1-(1/N) respectively For each host in P2P networks . so the probability that $\sum_{i \in V(t)} d_i$ attacks do not take place for each host is $(1 - 1/N)^{\sum_{i \in V(t)} d_i}$. Thus, the probability that at least one attack of $\sum_{i \in V(t)} d_i$ attacks is occurred is equal to $(1 - 1/N)^{\sum_{i \in V(t)} d_i}$. the probability of belonging to a susceptible population is $\frac{S(t)}{N}$ For each host and infection probability is $1 - \delta$ if each susceptible host is attacked . Then variation in the number of infected hosts on period (t, t+1) converted from susceptible hosts is equal to

$$S(t) \times (1-\delta) \times \left[1 - (1 - \frac{1}{N})\right]^{\sum_{i \in V(t)} d_i} \qquad (17)$$

infected population increases by infection process and is reduces by immunization process . so change in I(t) on period (t t+1) is :

$$I(t+1) - I(t) = S(t) \times (1-\delta) \times \left[1 - \left(1 - \frac{1}{N}\right)^{\sum di}\right] - \left[R(t+1) - R(t)\right] \qquad (18)$$

Susceptible population is reduced also by infection and immunization process . Thus change in S(t) on period (t t+1) is :

$$S(t+1) - S(t) = -S(t) \times (1-\delta) \times \left[1 - \left(1 - \frac{1}{N}\right)^{\sum di}\right] - \left[Q(t+1) - Q(t)\right] \qquad (19)$$

It is agreed that change of R(t) in SIR and two-factor model only depends on I(t) and infected hosts removed population change discrete form on period (t t+1) as the following equation :

$$R(t+1) - R(t) = \lambda_{ir} I(t) \qquad (20)$$

cleaning process in four-factor model is similar to two-factor classic model . hence, giving the details of modeling of from R(t) and Q(t) change is not necessary . Discrete form of removed population change from susceptible hosts on period (t t+1) is :

$$Q(t+1) - Q(t) = \lambda_{sr} S(t) J(t) \qquad (21)$$

substitution of equations into each other , obtained equations are :

$$\frac{dI(t)}{dt} = \frac{dS(t)}{dt} \times (1-\delta) \times \left[1 - \left(1 - \frac{1}{N}\right)^{\sum d_i}\right] - \frac{dR(t)}{dt} \qquad (22)$$

$$\frac{dS(t)}{dt} = -\frac{dS(t)}{dt} \times (1-\delta) \times \left[1 - \left(1 - \frac{1}{N}\right)^{\sum d_i}\right] - \frac{dQ(t)}{dt} \qquad (23)$$

$$\frac{dR(t)}{dt} = \lambda_{sr} S(t) - \lambda_{ir} I(t) \qquad (24)$$

$$\frac{dQ(t)}{dt} = \lambda_{sr} S(t) J(t) \qquad (25)$$

$$J(t) = I(t) + R(t) \quad (26)$$

$$N = S(t) + I(t) + R(t) + Q(t) \quad (27)$$

At first $R(0) = 0$ and at the beginning of worm propagation $I(0) = I_0 \ll N$ and most of the users are not informed of the worm . Hence, removing processes of infected population is neglected .here $Q(0)$ is adjusted as Q0 or 0 because some of the hosts can immune themselves against attacks by various security techniques as antivirus, firewall and personal systems . so it is needed to immunized hosts to have removed (cleaned) state at the beginning of the worm propagation .As it is observed proposed model makes results close to real by considering most important parameters such as bandwidth and infected and not infected file sizes .Also this method retrieves the lack of dynamism of two-factor and four-factor models .To investigate the validity of the formulas, simulation is presented in numerical values . this is why Peersim simulator software is used .This software's data are plotted with MATLAB simulation.

3. Simulation

In this part the propagation of proactive worms with various parameters and under various conditions is investigated . The initial values of the parameters are listed in table I . The parameters that are not listed in Table II are zero as default . The important point is that the degree of each peer is N-1, as it is considered that communication in each network is complete .

Table II : initial values of some simulated parameters

S(0)	I(0)	S_i	S_{ui}	Bw	λ_{sr}	λ_{ir}	λ_{is}	c	Q(0)	R(0)	δ
10000	10	100	1000	32	0.001	0.002	0.001	10	0	0	**1**

3.1 Models evaluation

curve of the number of infected, susceptible and recovered peers based on time units with parameters default values are depicted in Fig.3 .

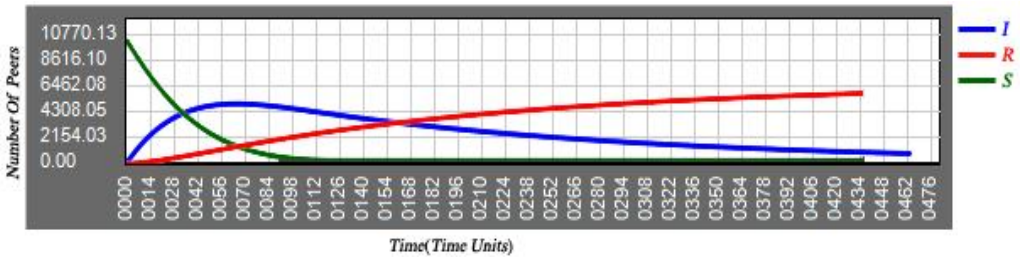

Figure 3 : number of infected, susceptible, recovered peers

As it is seen on the curve the number of infected peers is reduced over the time . In other words, over the time, the peers have been immunized with the rate λ_{ir} resulted in increasing recovered peers and reducing infected peers . the effect of other parameters in this model is investigated as follows .

3.2 Average parameter of infected file size (S_i)

The effect of infected files size on number of infected peers is shown in Fig.4 .

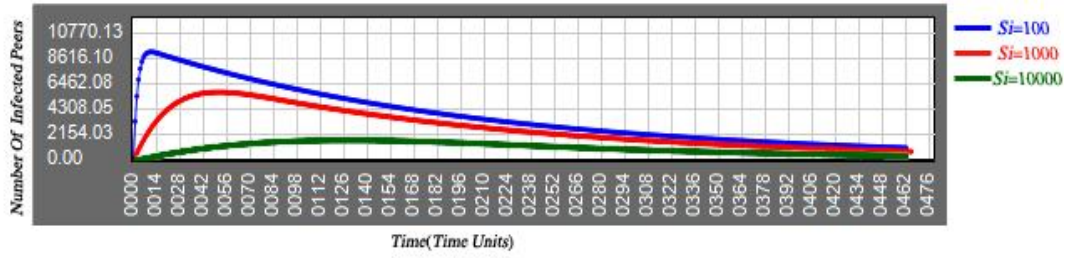

Figure 4 : effect of infected files on the number of infected peers

Simulation is performed using three distinct file size as it is presented in table III .

Table III : File size influence on percent of infected peers

File size (KB)	Time unit	Infection percent
100	10	91%
1000	40	57%
10000	100	16%

This simulation is performed with three different sizes . the result is that as the file size gets bigger , the propagation rate becomes slower . this is due to reduction of downloading rate by increasing infected file size . this simulation indicates that Band width influence on propagation rate is not negligible which is not considered in previous models .

3.3 The average parameter of uninfected file size (S_{ui})

Figure 5 illustrates the effect of uninfected files size on number of infected peers .

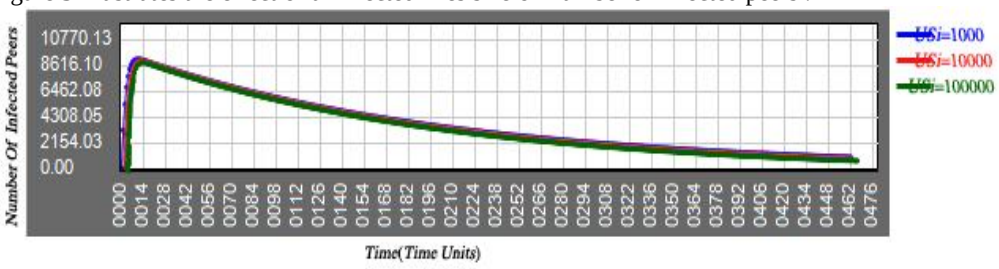

Figure 5 : effect of uninfected files size on the number of infected peers curve

As it is shown in the fig.4 , the size of uninfected files doesn't influence the propagation process . since there is no requirement to download the file by users in proactive worms' propagation . Thus, proactive worms don't propagate uninfected files . it will be obtained another result if simulation is performed on passive worms propagation .

3.4 Bandwidth parameter (bw)

Figure 6 shows the effect of bandwidth on number of infected peers .

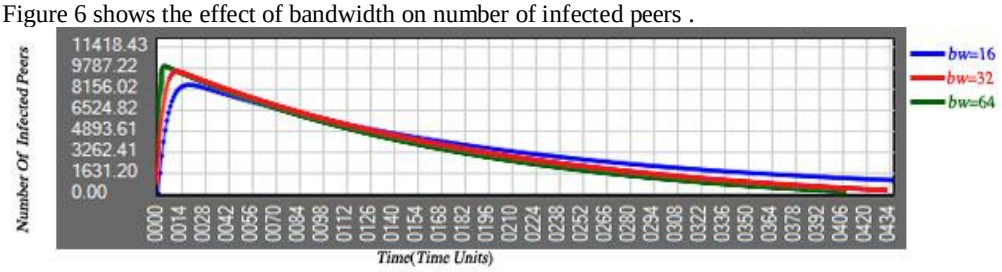

Figure 6 : effect of band width on the number of infected peers

Influence of Band width on peer infection is illustrated in table IV . bandwidth changing eventuated Interesting results . As Fig.5 shows , bandwidth has maximum influence on propagation speed among other parameters . download rate increases By increasing bandwidth and propagation rate is more rapid than before . simulation performed with bandwidths higher than 256 and there were no considerable differences with this one . It seems that the infected file size should be effectual when the bandwidth is higher .

Table IV : Band width efficacy on peer infection

Band width	Time unit	Infection percent
16	18	84%
32	10	91%
64	6	95%

3.5 Susceptible peers variations

Fig.7 depicts Susceptible peers variations . the most important point of that is high infection rate . as it can be seen , at t=0 there are 10000 susceptible peers which falls down almost to zero at just 17 time units . this indicates the extra high propagation speed in the proposed MPropagation model . So Band width and infected file size are very influential on propagation speed .

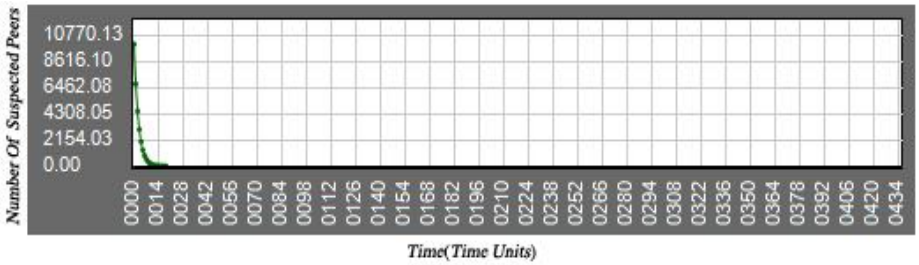

Figure 7 : Susceptible peers variations influence on infection rate

4. Conclusion

In this paper four-factor and similar models are analyzed . Then new propagation model called MPropagation presented . its performance was close to real operational environment. Because important parameters as bandwidth of network and average infected and non-infected file sizes is considered to make the simulation results close to reality . infected files size is considered 100 kilobytes .this is close to value in real world and it caused the propagation speed increasing . Peersim software is used to simulate proposed model .One of the advantages of this software is high level of its programming language makes its simple to understand . it has ability of high variety .

REFERENCES

[1] D. M. Kienzle and M. C. Elder, "Recent worms: a survey and trends," 2003, pp. 1-10.

[2] Q. Sun, Q. Wang, and J. Ren, "Modeling and analysis of the proactive worm in unstructured Peer-to-Peer Network," *Journal of Convergence Information Technology,* vol. 5, pp. 111-117, 2010.

[3] A. Kalafut, A. Acharya, and M. Gupta, "A study of malware in peer-to-peer networks," 2006, pp. 327-332.

[4] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa, and S. Chien, "A first look at peer-to-peer worms: Threats and defenses," *Peer-to-Peer Systems IV,* pp. 24-35, 2005.

[5] J. K. K. Lakshminarayanan, "Implications of peer-to-peer networks on worm attacks and defenses," Tech. Rep., UCB2003.

[6] J. Ma, X. Chen, and G. Xiang, "Modeling passive worm propagation in peer-to-peer system," 2006, pp. 1129-1132.

[7] Y. Zhang, Z. Li, Z. Hu, Q. Huang, and C. Lu, "Evolutionary proactive P2P worm: Propagation modeling and simulation," 2008, pp. 261-264.

[8] J. Luo, B. Xiao, G. Liu, Q. Xiao, and S. Zhou, "Modeling and analysis of self-stopping BTWorms using dynamic hit list in P2P networks," 2009, pp. 1-8.

[9] X. Fan, W. W. Guo, and M. Looi, "Modeling and Simulating the Propagation of Unstructured Peer-to-Peer Worms," 2011, pp. 573-577.

[10] X. Zhang, T. Chen, J. Zheng, and H. Li, "Proactive worm propagation modeling and analysis in unstructured peer-to-peer networks," *Journal of Zhejiang University-Science C,* vol. 11, pp. 119-129, 2010.

[11] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," 2002, pp. 138-147.

[12] W. Yu, S. Chellappan, X. Wang, and D. Xuan, "Peer-to-peer system-based active worm attacks: Modeling, analysis and defense," *Computer Communications,* vol. 31, pp. 4005-4017, 2008.

[13] C. Feng, Z. Qin, L. Cuthbet, and L. Tokarchuk, "Propagation model of active worms in P2P networks," 2008, pp. 1908-1912.

[14] Y. Zhou, Z. F. Wu, H. Wang, J. Zhong, Y. Feng, and Z. Z. Zhu, "Breaking monocultures in P2P networks for worm prevention," 2006, pp. 2793-2798.

[15] D. McIlwraith, M. Paquier, and E. Kotsovinos, "di-jest: Autonomic neighbour management for worm resilience in p2p systems," 2008, pp. 1-6.

[16] C. C. Zou, D. Towsley, W. Gong, and S. Cai, "Routing worm: A fast, selective attack worm based on ip address information," 2005, pp. 199-206.

[17] X. Nie, Y. Wang, J. Jing, and Q. Liu, "Understanding the impact of overlay topologies on peer-to-peer worm propagation," 2008, pp. 863-867.

[18] e. D. S. a. (2001). *Code Red Worm* Available at http://www.eeye.com/html/Research/ Advisories/AL20010804.html.

[19] e. D. S. b. (2001). *Code Red II Worm* Available at http://www.eeye.com/html/Research/ Advisories/AL20010804.html.

[20] Y. Wang, S. Wen, S. Cesare, W. Zhou, and Y. Xiang, "Eliminating Errors in Worm Propagation Models," *Communications Letters, IEEE*, pp. 1-3, 2011.

[21] Z. Chen and C. Ji, "Spatial-temporal modeling of malware propagation in networks," *Neural Networks, IEEE Transactions on*, vol. 16, pp. 1291-1303, 2005.

[22] C. Feng, Z. Qin, L. Cuthbet, and L. Tokarchuk, "Propagation modeling of passive worms in P2P networks," 2008, pp. 1027-1031.