J Comput Virol (2009) 5:357–364
DOI 10.1007/s11416-008-0099-8

EICAR 2008 EXTENDED VERSION

Treating scalability and modelling human countermeasures against local preference worms via gradient models

Markos Avlonitis · Emmanouil Magkos · Michalis Stefanidakis · Vassilis Chrissikopoulos

Received: 20 January 2008 / Revised: 1 July 2008 / Accepted: 8 July 2008 / Published online: 23 July 2008

Abstract A network worm is a specific type of malicious software that self propagates by exploiting application vulnerabilities in network-connected systems. Worm propagation models are mathematical models that attempt to capture the propagation dynamics of scanning worms as a means to understand their behaviour. It turns out that the emerged scalability in worm propagation plays an important role in order to describe the propagation in a realistic way. On the other hand human-based countermeasures also drastically affect the propagation in time and space. This work elaborates on a recent propagation model (Avlonitis et al. in J Comput Virol 3, 87–92, 2007) that makes use of Partial Differential Equations in order to treat correctly scalability and non-uniform behaviour (e.g., local preference worms). The aforementioned gradient model is extended in order to take into account human-based countermeasures that influence the propagation of local-preference worms in the Internet. Certain aspects of scalability emerged in random and local preference strategies are also discussed by means of random field considerations. As a result the size of a critical network that needs to be studied in order to describe the global propagation of a scanning worm is estimated. Finally, we present simulation results that validate the proposed analytical results and demonstrate the higher propagation rate of local preference worms compared with random scanning worms.

M. Avlonitis · E. Magkos (✉) · M. Stefanidakis · V. Chrissikopoulos
Department of Informatics, Ionian University,
Plateia Tsirigoti 7, 49100 Kerkyra, Greece
e-mail: emagos@ionio.gr

M. Avlonitis
e-mail: avlon@ionio.gr

M. Stefanidakis
e-mail: mistral@ionio.gr

V. Chrissikopoulos
e-mail: vchris@ionio.gr

1 Introduction

A network worm is a specific type of malicious software that self propagates by exploiting application vulnerabilities in network-connected systems. During recent years, several worms have caused significant damage in corporate and Internet core networks [2–6]. While early worms followed rather random spread patterns and aimed mostly at Denial of Service attacks, future worms are expected to adopt advanced scanning strategies and even bear a catastrophic payload [7–10]. A fast spreading worm armed with a priori information about the distribution of vulnerable nodes in the underlying infrastructure [10] may also perform targeted attacks and bring down the majority of the target networks within a short time interval. Securing networks against worm attacks is particularly important for critical infrastructure applications, such as banking and financial applications, emergency deployment services and military applications.

Among the various strategies that worms can follow for scanning vulnerable hosts [7,11] two strategies have been primarily considered: a) *random scanning worms* (e.g., Code Red I [3], Slammer [4]) uniformly scan the 32-bit IP address space to find and infect vulnerable targets; b) *local preference worms* (e.g., Blaster [5], Coder Red II [3], Nimda [2]) preferably infect "neighbouring" hosts (e.g., within a specific /8, /16 or /24 address block) within a network. It has been shown that local preference worms spread faster, compared to random scanning worms, when the vulnerable hosts in the Internet are unevenly distributed, which is a realistic assumption [10]. Such network-aware worms tend to infect clusters of nodes, often with similar application vulnerabilities, before moving to other networks. It is also expected that in the future, when the IPv6 will be a reality, local preference may be an optimal scanning strategy for worms, given the infeasibility of randomly scanning the entire 128-bit address space [12].

From a security point of view, most traditional techniques for controlling worm intrusions involve human intervention and are mainly *preventive* (e.g., firewall policies and network perimeter, patch strategies, network segmentation, updating virus scanners, removing hosts from the network), aiming at reducing the risk of infection from a scanning worm. Some of these could also be seen as reactive measures that aim to reduce the exposure of a network to an already active worm. Recently, much attention has also been shed on *detection* measures with automated real-time monitoring. Detection strategies can also be categorized into local and global strategies. For example, Intrusion Detection Systems (IDS) can be used to detect traffic anomalies in the internal network [13–15]. While such local monitoring strategies can be effective in early detecting and raise threshold alarms within an organization, they may not be able to capture the global behaviour of a worm in the Internet, due to the heterogeneity of the various local networks. On the other hand, a global monitoring strategy often uses a centrally controlled Internet infrastructure which gathers log data from geographically distributed systems. Such strategies make use of highly distributed network telescopes or honeypots to attract and identify attackers [16]. Admittedly it also seems difficult to setup global monitoring infrastructures that require a very large monitored network to become effective [13].

Worm propagation models are epidemiological models that capture the propagation dynamics of scanning worms as a means to understand the behaviour of various worm types. Studying the behaviour of a scanning worm can also help towards designing and evaluating strategies for monitoring and early detection, as well as predicting the time limits for early response. While it seems hard to create realistic models mainly due to the heterogeneity of the Internet networks, recent analytical models (e.g., [7,17]) have been validated with simulation results that approximate the behaviour of random scanning worms such as the Code Red and Slammer worms, for which real measurements are disposable on the Internet. Worm propagation models extend the classical epidemiological model [18] to describe the behaviour of a worm. The first complete application of mathematical models to computer virus propagation was proposed in [19]. Traditionally, propagation models are given names according to the possible states of the host population. For example, the simple epidemic model in [7] is a SI (Susceptible-Infected) model which describes random scanning worms that peak before a remedy is deployed. This model was extended in [17] to include hosts that are Recovered (i.e., a SIR model) for example as a result of installing a patch or a virus scanner. The work in [11] also modelled local preference worms following the SI approach. In another example, a model where susceptible hosts can become infected and then go back to a susceptible state (e.g., as a result of resetting a system where the propagation code resides in the main memory), is called a SIS model [16]. Other models take into account the fact that nodes can be isolated (e.g., powered down or quarantined) in an attempt to mitigate the worm propagation (e.g., [20]). Furthermore, there are models that attempt to take into account various non-uniformities of the underlying networks: for example, worm propagation may be influenced by bandwidth variations and congestion [16,21,22] or by the non-uniform behaviour of the worm itself (e.g., a worm with varying scan rate) [14].

To the best of our knowledge, most worm propagation models found in the literature make use of *Ordinary Differential Equations* (ODE) to describe the phenomenon. Unfortunately, results based on ODEs do not describe the spatial behaviour of the worm propagation phenomena, and thus do not properly address scalability issues (e.g., an ODE model will fail to tell how infected a specific area in space becomes). In a recent model proposed in [1] the classical model was extended by incorporating spatial interactions between and within networks and an evolution equation for worm propagation into an arbitrary subnet was proposed. According to the formalism, the notion of a critical network size (hereinafter called a *critical network*) was also introduced. It was suggested that the worm propagation within such a critical network may be considered in order to predict the global propagation of the worm in the Internet. The formalism can take into account non-uniformities that are due either to local interactions between neighbouring subnets (e.g., as a result of a local preference strategy) or to the heterogeneity of the underlying infrastructure, (e.g., bandwidth variations, different topologies, human countermeasures etc.).

Our Contribution. In this work we elaborate on the recent gradient model of [1] by introducing an appropriate new term which models human intervention (i.e., preventive and/or reactive measures that mitigate the worm propagation), thus better approximating the real-world behaviour of scanning worms and of the host population in the Internet. Furthermore, we study the dynamics of the new model and give an emphasis to explaining the higher propagation rates of local-preference worm strategies (as observed in real measurements), compared with the propagation rates of random scanning worms. Moreover, the powerfulness of gradient models to describe scalability of worm propagation in terms of spatiotemporal interactions between infected hosts, is demonstrated. It is claimed that the gradient models point towards a theory of scalability which is missing from the literature on worm propagation. Finally, we make use of random field considerations in order to estimate the size of a critical network, which needs to be studied in order to describe the global propagation of a scanning worm. Throughout the paper, we validate our estimates and analytical results with simulation outcomes.

Organization of the paper. In Sect. 2 we briefly present the results of the approach in [1]. In Sect. 3 we make

random field considerations to estimate the size of the critical network. In Sect. 4 we present a new model that incorporates human intervention in the model of [1], and analytically solve our equations. In Sect. 5 we present simulation results that validate our theoretical estimates, while Sect. 6 concludes the paper.

2 A brief review of the gradient model

This section briefly describes the model proposed in [1]. Let N_i be the number of susceptible hosts in the i-th subnet and I_i the infected hosts in the same subnet. Suppose that K is the average propagation speed of the worm and in a first approximation let us say that it is constant in every single subnet. Assuming a random scanning strategy, there is a probability P_{IN} that a host inside the subnet targets a host inside the same subnet and a probability P_{OUT} that instead it attacks another subnet. Following the line of [1], starting from a continuous evolution equation of the form,

$$\frac{da(x,t)}{dt} = K\frac{N_s}{N}(1-a(x,t))\left[\int a(y,t)dy\right] \tag{1}$$

and using a Taylor expansion around x ($y = x + r$), we end up with a spatial generalization of the simple epidemic model (in order to capture interactions between subnets either due to Internet non-uniformities or due to non-uniform scanning strategies)

$$\frac{da_X}{dt} = K\frac{N_s}{N}(1-a_X)\int\left(a_X + r\frac{\vartheta a_X}{\vartheta x} + \frac{1}{2}r^2\frac{\vartheta^2 a_X}{\vartheta x^2}\right)dr \tag{2}$$

where $a_X = a(x,t)$ is the fraction of the infected hosts, $n = N_{Total}/Ns$ is the number of subnets in the Internet which has a total of N_{Total} susceptible hosts and N_s is the size of the subnets.

Assuming a uniform scanning strategy and a homogeneous network infrastructure, the number of infected hosts uniformly increases within the Internet. As a result a uniform spatial distribution emerges and the spatial partial derivatives in Eq. (2) vanish. In this scenario the following evolution equations were derived,

$$\frac{da_X}{dt} = Ka_X(1-a_X) \tag{3}$$

$$\frac{da}{dt} = Ka(1-a) \tag{4}$$

where $a = (1/N_{Total})\int_n N_S a_X dr$ is the total or average density of infected hosts in the Internet.

Comparing Eqs. (3) and (4) it is clear that when no non-uniformities are present, the average behaviour of a worm population in the Internet coincides with its behaviour in any network of arbitrary size (the smallest size limited to scales where discrete behaviour is not present).

When a local preference scanning strategy is assumed, there is a uniform probability to scan addresses in the same "/m" prefix network. As a result a non-uniform distribution of infected hosts emerges and the spatial derivatives in Eq. (2) are no longer negligible. The following evolution equation holds,

$$\frac{da_X}{dt} = N_s(1-a_X)\left\{\left[\beta' + (Q-1)\beta''\right]a_X + \beta' c\frac{\vartheta^2 a_X}{\vartheta x^2}\right\} \tag{5}$$

where $\beta = \eta/\Omega$ is called the pairwise rate of infection (η is an average scan rate and Ω is the total number of IP addresses), β' and β'' are pairwise rates of infection in local and remote scan respectively ($\beta' = p\eta/2^{32-m}$, $\beta'' = (1-p)\eta/(Q-1)2^{32-m}$ where Q is the number of "/m" prefix networks in Ω) and $c = (1/2)\int_{Q_x} r^2 dr$. Eq. (5) provides a specific law of worm propagation for a local preference scanning strategy taking into account the resulting heterogeneities.

Our formalism introduces as a crucial model parameter, the gradient coefficient c which is a measure of the size of the *critical network*, i.e., a representative neighbourhood of subnets. This means that in a neighbourhood of this scale the worm population proceeds independently. As a result, the evolution of the worm population within the critical network coincides with the evolution of the population in the Internet as a whole. In Sect. 3 we use random field considerations to provide an estimate on the critical network size. Furthermore, while the spatial model proposed by [1] is able to take into account and model interactions between infected hosts, thus introducing the notion and existence of a critical network, no effort has been given to incorporate a number of factors that influence the propagation of a worm in the Internet, such as human intervention, e.g., preventive and reactive measures against scanning worms. In Sect. 4 we will incorporate such human-based actions in order to achieve a more realistic understanding of local preference worm propagation strategies in the Internet.

3 Random field considerations

It is well known that either in physical or in artificial systems, complex dynamics may emerge due to multiple or long range interactions. As a result, complex structures are developed and a variety of critical phenomena may arise. In this context, worm propagation in the Internet may be viewed as an artificial dynamic system the evolution of which could be affected by random and/or scale effects.

In order to examine these dynamics and especially the spatial behaviour of worm propagation in the Internet, we

may apply well established tools of statistical methods from other fields. The connection with the formalism proposed in [1] is based on the underlying idea that it is possible to describe the average worm behaviour in a deterministic way, by considering a critical scale of network size. In this critical scale, it is possible to write down an evolution equation (e.g., Eq. (5)) where the random effects in scales below that size (e.g., in smaller subnets), can be taken into account with the introduction of the appropriate gradient terms. At this point, a crucial question arises, i.e., whether there is such a scale or an hierarchy of scales emerges.

In the context of probability theory the above question can be treated with the notion of *moving averages* [23] and the existence or not of the corresponding correlation length. From a stationary random process $r(x)$ with mean $\bar{r}$ and variance s^2 a family of moving average processes $r_T(x)$ may be obtained as

$$r_T(x) = \frac{1}{T}\int_{x-T/2}^{x+T/2} r(x)dx \tag{6}$$

where T denotes the averaging "window" in space. We define the variance function $\gamma(T) = s_T^2/s^2$ as the ratio of the variances of the resulting average pattern (after smoothing with average window T) over the original one. Then for a general class of processes the following relation holds (m is a pattern parameter and λ is the corresponding correlation length of the pattern)

$$\gamma(T) = \left[1 + (\frac{\lambda}{T})^m\right]^{-1/m} \tag{7}$$

or for fractal patterns (b is a parameter correlated to the fractal dimension)

$$\gamma(T) \propto T^{-b} \tag{8}$$

As a result given the spatial pattern of worm propagation in the Internet (this consists of a sequence of 0's for non infected hosts and 1's for infected hosts) we can estimate pattern data points using the definition $\gamma(T) = s_T^2/s^2$. Plotting these points and fitting the curve of Eqs. (7, 8) we may estimate the curve parameters λ, m or b. This procedure is depicted in Fig. 1 for random scanning and Fig. 2 for local preference, where the spatial pattern was taken from simulation results. Solid curves in both figures represent a *power law* behaviour. It is evident that in the case of random scanning the resulting worm propagation pattern over the Internet is a fractal and, as also predicted in [1], the evolution of the worm population in any size of selected subnets (the only limitation is to be large enough so that the phenomenon is not discrete) coincides with the evolution of the worm population in the Internet. On the other hand, in case of a local preference strategy this result breaks down. Indeed, as can be seen in Fig. 2 the power law behaviour does not fit correctly the simulation data. In this case, exponential-like variance functions of the form of Eq. (7) are more appropriate.

This result is an evidence for the existence of a *correlation length* of the worm pattern in the Internet. In probability theory this defines a critical scale of fluctuations which coincides with the critical network size in our analysis. Below that scale worm propagation is affected by the interactions from neighbouring hosts while for scales above the critical one, worm propagation proceeds independently. Again these findings confirm the results suggested in [1].

Note that our simulation for local preference was based on a Blaster-like worm, where the worm targeted neighbouring nodes with 60% probability, while performing random

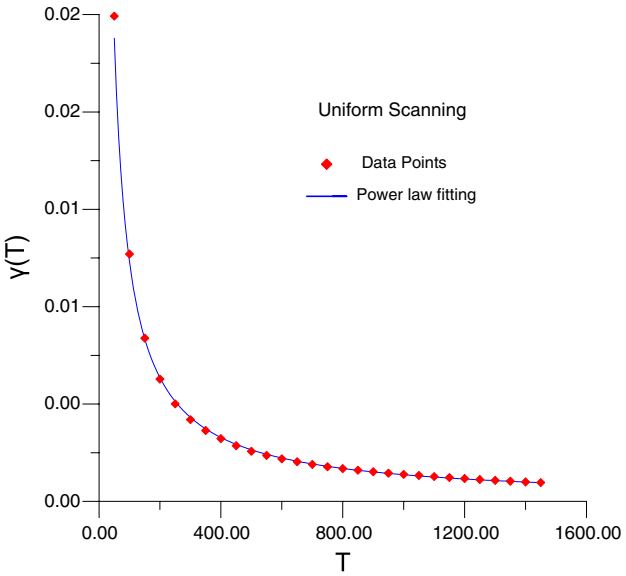

Fig. 1 Estimated variance function for random scanning

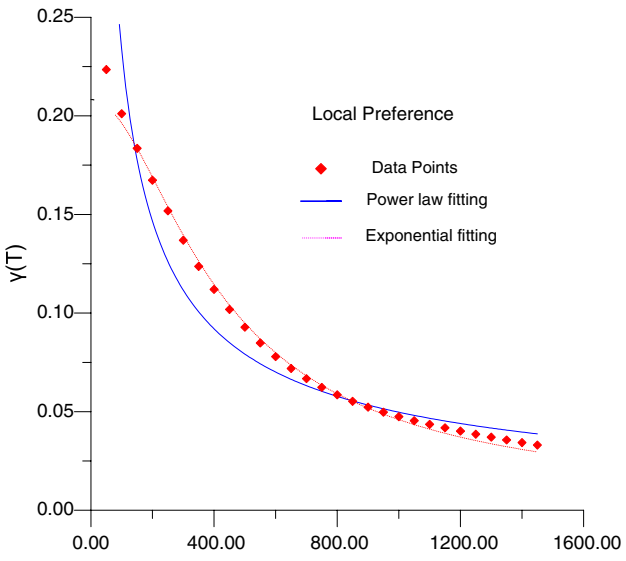

Fig. 2 Estimated variance function for local preference scanning

scanning with a probability of 40%. This means that the resulting pattern consists of the interplay of two evolution dynamics. In a first approximation, fitting the simulation data in Fig. 2, our analysis demonstrates the existence of a correlation length of the order of 170 for local preference. Taking into account that there is a linear relation between this correlation length and the size of the critical network (the coefficient being of the order of four) a value of 700 hosts is finally estimated as the size of the critical network.

Given the limitations of our approach, the values of the size of a critical network are of great significance. The knowledge of such values could be used to fill the gap between local and global monitoring strategies so that a representative neighborhood of subnets could be used in order to study the global behaviour of a worm in an effective and affordable way.

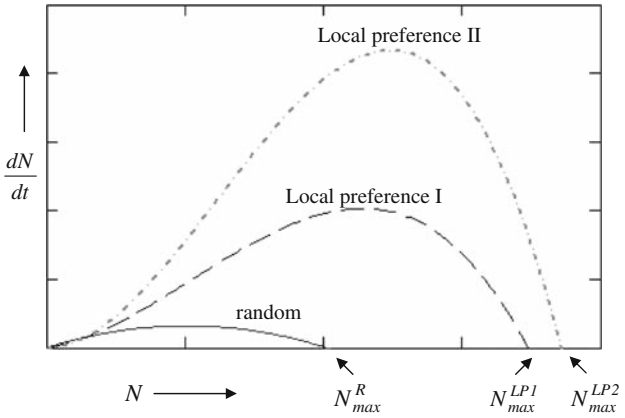

Fig. 3 Approximating analytical results of the gradient model with a loss term

4 Incorporating human intervention in worm propagation

In order to take into account human intervention in local preference scan strategies in the initial model proposed in Eq. (5) it is necessary to introduce an appropriate *loss term*. The following gradient model is proposed,

$$\frac{da_X}{dt} = K' a_X(1 - a_X) - g(a_X) + c'(a_X)\frac{\vartheta^2 a_X}{\vartheta x^2} \tag{9}$$

where the abbreviations for the rate $K' = N_S[\beta' + (Q-1)\beta'']$ and the gradient coefficient $c'(a_X) = \beta' N_S(1 - a_X)c$ was used while the new term $g(a_X)$ models human intervention. The following analytical form for $g(a_X)$ is adopted,

$$g(a_X) = g_1 \frac{a_X^2}{g_2^2 + a_X^2} \tag{10}$$

where $g_1.g_2$ are appropriate constants. This kind of loss term was previously used in other fields in order to model population dynamics (e.g., [24]). The following properties hold: for early spread, i.e., for $a_X \to 0$, $g(a_X) \simeq a_X^2$ which is equivalent to say that initially the reduction of infected hosts is very low, while near saturation $a_X \to 1$, $g(a_X) \simeq g_1$, i.e., the rate of reduction of infected hosts reaches a high constant rate at a specific time after the release of the worm. This kind of behaviour is appropriate for worm spreading problems since in the real word, not too many hosts are initially aware of the presence of a new worm and as a result little effort is paid to mitigating its propagation. On the contrary, in the course of time more and more hosts are aware of the worm spreading and appropriate actions (both preventive and reactive) usually take place.

In order to evaluate the role of the proposed model in Eq. (10), and especially the role of the gradient term (which models local preference worm strategies) in the worm's propagation rate, the two versions of Eq. (10) with and without the gradient term, are considered. Furthermore, it is assumed that initially a more or less uniform distribution of nuclei of infected hosts emerge in the network (this is equivalent to assuming a quite common spatial solution of the form $a_X(x) = [Bcosh(x/A)]^{-2}$ emerges independently in each critical network, see for example in [25]). For this scenario and for the initial time states (*i.e.*, for $a_X \to 0$, $g(a_X) \simeq a_X^2$) of worm spreading, the time derivatives of Eq. (10) with and without the gradient term are depicted in Fig. 3, for arbitrary model parameters.

It can be seen that when a random scanning strategy is adopted then the corresponding model without the gradient term shows a low overall propagation rate while for a local preference strategy the corresponding model with the gradient term shows a higher overall propagation rate. As a consequence, the depicted analytical results confirm real measurements for local preference worms, which report faster propagation rates compared with random scanning worms. Moreover, recalling that $c'(a_X) = \beta' N_S(1 - a_X)c$, the stronger the local preference behaviour the higher contribution of the gradient term *e.g.*, the faster propagation rate as depicted with the dashed curves in Fig. 3.

Furthermore, the analytical results depicted in Fig. 3, show that the dynamic without the gradient term (*e.g.*, random scanning) reaches a maximum number of infected hosts N^R_{max} which is considerably lower than that reached when the gradient term enters the dynamics, N^{LP1}_{max} or N^{LP2}_{max} (local preference strategy). Thus, another outcome of the proposed model is that a local preference strategy not only obtains higher propagation rate but also results in much higher damage in the network.

However, as one of the main results of the present work, it is noted that human intervention during worm spreading can be modelled and quantified in the framework of the proposed model by means of only three model parameters, mainly g_1, g_2, N_S. This is not always an easy task and appropriate

values can be estimated only by calibrating model behaviour with real data. The powerfulness of the new model is that the calibration can be done at the beginning of worm propagation. As a result it may be possible to predict on time the future behaviour of the worm. For a robust calibration one should note that the new introduced term $g(a_X)$ captures healing of hosts that return, for some reason, to a susceptible state (*i.e.*, hosts that follow the SIS model). In order to incorporate other preventive and/or reactive countermeasures (*e.g.*, firewall policies, patch strategies, updating virus scanners or removing hosts from the network), a dynamic reduction of the size N_S of the susceptible hosts in Eq. (10) must be considered.

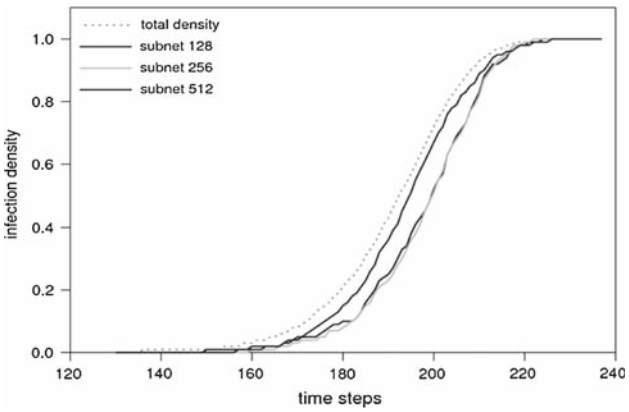

Fig. 4 Infection density in arbitrary probing subnets compared to global density

5 Exploring scalability in local preference strategies

As pointed out earlier, the so called gradient model for local preference worm strategies is able to capture the spatial behaviour of spreading worms. This can be done by means of a characteristic length entering to the corresponding gradient coefficient. The origin of this characteristic length relies on the interactions between hosts and determines the size of the critical network. Note that the smaller the gradient coefficient the smaller the characteristic length, *e.g.*, the smaller the size of the critical network. Once more here it is emphasized that the existence of a critical network guaranties that an observation of the worm propagation within the critical network may lead to a robust measure of the worm propagation in the entire network. As a result, in the framework of gradient models there is the possibility to address scalability analytically and further it is possible to measure (and quantify) the effect of the critical network size to worm propagation behaviour.

Under this interpretation, the proposed model in this work suggests that during worm propagation the characteristic length of the dynamics of the system changes since $c'(a_X) = \beta' N_S(1 - a_X)c$ is a function of a_X. Furthermore, the model predicts that initially a critical network for robust monitoring of worm propagation has a maximum size (since $c'(a_X)$ is maximum for $a_X \to 0$) and in the course of time this decreases and finally for $a_X \to 1$ the spreading behaviour coincides with a random scan strategy. This is an unexpected result and it is demonstrated later in this section by means of simulation results. Intuitively this can be understood since, in local preference scanning strategies, initially the density of infected hosts proceeds heterogeneously, while as the network goes to saturation the density of infected hosts tends to be homogeneous, *e.g.*, at any subnet it is almost equal to unity.

In order to verify the predictions of the proposed model presented in the previous and current sections, a simple discrete event simulator has been built. This setup is equivalent to a /16 network, describing a total number of 256 LAN clusters with each LAN having 256 hosts. All hosts are initially susceptible to worm infection and a single host in an arbitrary LAN is in infected state. The simulated worm performs 1 infection probe per time unit, something that leads to a rough correspondence of 1 ms per time step. Connection establishment delays are disregarded, as a UDP packet scanning method is assumed to be used. The simulator distinguishes between two types of probe propagation delays: 10 time units for intra-LAN and 100 time units for inter-LAN infection propagation.

In the first phase of simulation, a local preference strategy for address scanning was selected. No human countermeasures were accounted for, enabling thus the isolation and validation of the gradient term of the model-theoretical analysis. Probing subnets of various sizes have been used, containing part of, total, or aggregation of LANs with 128, 256 or 512 host per subnet, accordingly.

In Figure 4, the evolution of infection density of arbitrary selected subnets is compared to the global infection density evolution of the whole simulated setup. During the outbreak phase of the worm infection, locally probed estimations of the infection are not following accurately the global infection numbers. In the case of subnets with size 128 or 256 probes (that is, probing was accomplished within a sole LAN), there appears an average error of 40% in the estimation of the global infection density. When a critical size of 512 hosts is considered, involving the aggregation of 2 LANs in a probing subnet, the corresponding estimation error is of the order of 15%. On the other hand, near the saturation phase of infection, we observe that the behavior of the worm propagation in different size subnets coincides. This confirms the theoretical result stated earlier in this section, *i.e.*, that near the saturation local preference worms behave the same as random scanning worms.

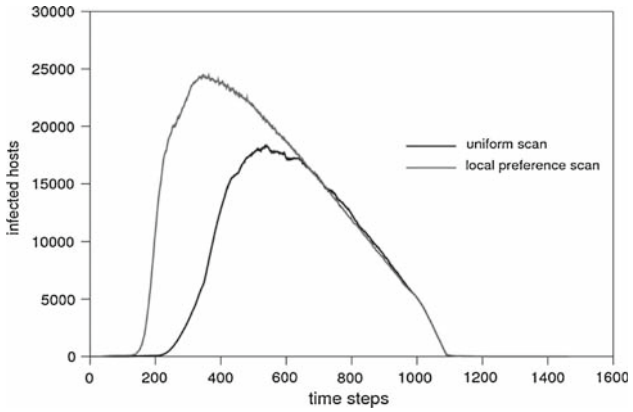

Fig. 5 Number of infected hosts in total simulated setup

In the second part of simulation experiments, a constant rate of one per thousand of the total number of hosts is assumed to be immunized in each time step, accounting for preventive countermeasures in the setup. In order to capture the human initiated healing of infected hosts an additional disinfection action is performed in each time step, which returns a number of infected hosts to the susceptible state. This number of healed hosts per time step is proportional (one per thousand) to the square of infected hosts within a LAN cluster, as long as the number of infected hosts in the LAN is kept low, but stabilizes later at 0.25% when the number of infected hosts overpasses one half of the total available hosts in the LAN.

Two distinct cases of address scanning strategies have been simulated: In the first case, the generated addresses have a uniform (random) distribution, disregarding any information about locality of LAN clusters. Each infection probe can target any other host in the entire simulated setup with equal probability. In the second case, the worm exhibits a local preference in the probe addresses it generates. Following the characteristics of a Blaster-like worm, 40% of the generated addresses target other hosts in the same LAN cluster, while the remaining 60% target hosts in random LANs.

In both cases, the evolution of the number of infected hosts through time is being tracked, in order to compare and validate the model-theoretically predicted behavior of worm propagation.

As depicted in simulation results of Fig. 5, the outbreak of infection is faster with the local preference scanning strategy and the peak value of infected hosts is higher compared to the relevant results of random scanning. The two simulation outcomes are with strict accordance to the model–theoretical predictions presented in Sect. 4. Moreover, it is clearly shown in Fig. 5 that the immunization constant rate procedure is the dominant characteristic after reaching peak values of infected hosts in both uniform and local preference cases. This leads to a similar ending phase of infection evolution.

6 Conclusions

The design of techniques and strategies for an effective, affordable and implementable resistance against future worms will be a research challenge in the years to come. Given the apparent inadequacy of existing proactive strategies to deal with advanced, fast spreading worms, monitoring and intrusion detection can be seen as another layer of protection, complementary to preventive and reactive security (e.g., firewall and disinfection technologies). IDS technology could take advantage of the knowledge gained by recent worm propagation models that attempt to describe how a worm is propagated, by using mathematical equations.

This work elaborated on a recent worm propagation model [1], where it was shown that there is a representative neighborhood of hosts of appropriate size over which the evolution of worm population follows correctly the evolution of the population in the Internet. More specifically, in this work a loss term is added to describe the reduction of the worm population, caused by preventive and/or reactive countermeasures. Furthermore, we explain analytically and then demonstrate, with simulation results, the fact that local preference worms spread faster and result in greater damage compared with random scanning worms. This work can be used to better describe the real-world behavior of local preference scanning worms in the Internet.

Finally, a theoretical framework for addressing scalability of worm propagation in the Internet was proposed via gradient models. More specifically it was shown that a hierarchy of critical network sizes is present during local preference worm propagation. In general, it is stated that gradient models are a very valuable tool in order to address scalability. In order to understand this, note that the characteristics of scalability depend on the characteristics of worm propagation strategies and on the network infrastructure. On the other hand we show that those characteristics determine the expression of the corresponding gradient term. As a result, we believe that correct estimation of the gradient coefficient for a scanning worm could be used to predict its scaled propagation.

References

1. Avlonitis, M., Magkos, E., Stefanidakis, M., Chrissikopoulos, V.: A spatial stochastic model for worm propagation: scale effects. J. Comput. Virol. **3**, 87–92 (2007)
2. Cert/c, C.: Cert advisory ca-2001-26 nimda worm (2001)
3. Moore, D., Shannon, C., Claffy, K.C.: Code-red: a case study on the spread and victims of an internet worm. In: IMW'02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, pp. 273–284. ACM, New York (2002)
4. Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N.: Inside the slammer worm. IEEE Secur. Priv. **1**, 33–39 (2003)

5. Berghel, H.: Malware month. Commun. ACM **46**, 15–19 (2003)
6. Shannon, C., Moore, D.: The spread of the witty worm. IEEE Secur. Priv. **2**, 46–50 (2004)
7. Staniford, S., Paxson, V., Weaver, N.: How to own the internet in your spare time. In: Proceedings of the 11th USENIX Security Symposium, pp. 149–167. USENIX Association, Berkeley (2002)
8. Zou, C.C., Towsley, D., Gong, W., Cai, S.: Advanced routing worm and its security challenges. Simul. **82**, 75–85 (2006)
9. Wu, J., V.S.G.L., Kwiat, K.: An effective architecture and algorithm for detecting worms with various scan techniques. In: 11th Annual Network and Distributed System Security Symposium (NDSS'04), San Diego (2004)
10. Chen, Z., Chen, C., Ji, C.: Understanding localized-scanning worms. In: 26th IEEE International Performance Computing and Communications Conference, IPCCC 2007, pp. 186–193 (2007)
11. Zou, C.C., Towsley, D., Gong, W.: On the performance of internet worm scanning strategies. Perform. Eval. **63**, 700–723 (2006)
12. Keromytis, A.D., Bellovin, S.M., Cheswick, B.: Worm propagation strategies in an ipv6 internet. USENIX, Login **31**, 70–76 (2006)
13. Zou, C., Gong, W., Towsley, D., Gao, L.: The monitoring and early detection of internet worms. ACM Trans. Networking **13**, 961–974 (2005)
14. Yu, W., Wang, X., Xuan, D., Lee, D.: Effective detection of active worms with varying scan rate. International Conference on Security and Privacy in Communication Networks (IEEE SecureComm), pp. 1–10 (2006)
15. Morin, B., Mé, L.: Intrusion detection and virology: an analysis of differences, similarities and complementariness. J. Comput. Virol. **3**, 39–49 (2007)
16. Serazzi, G., Zanero, S.: Computer virus propagation models. In: MASCOTS Tutorials. Volume 2965 of Lecture Notes in Computer Science, pp. 26–50. Springer, Heidelberg (2003)
17. Zou, C.C., Gong, W., Towsley, D.: Code red worm propagation modeling and analysis. In: CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pp. 138–147. ACM, New York (2002)
18. Anderson, R.M., May, R.M.: Infectious diseases of humans: dynamics and control. Oxford Science Publications, (1992)
19. Kephart, J.O., White, S.R.: Directed-graph epidemiological models of computer viruses. In: IEEE Symposium on Security and Privacy, pp. 343–361 (1991)
20. Onwubiko, C., Lenaghan, A., Hebbes, L.: An improved worm mitigation model for evaluating the spread of aggressive network worms. Computer as a Tool, 2005. EUROCON 2005. Int. Conf. **2**, 1710–1713 (2005)
21. Wang, Y., Wang, C.: Modeling the effects of timing parameters on virus propagation. In: WORM '03: Proceedings of the 2003 ACM workshop on Rapid malcode, pp. 61–66. ACM, New York (2003)
22. Kesidis, G., Hamadeh, I., Jiwasurat, S.: Coupled kermack-mckendrick models for randomly scanning and bandwidth-saturating internet worms. In: Quality of Service in Multiservice IP Networks, Third International Workshop, QoS-IP 2005. Lecture Notes in Computer Science, vol. 3375, pp. 101–109. Springer, Heidelberg (2005)
23. Vanmarcke, E.: Random fields, analysis and synthesis. MIT Press, Cambridge (1983)
24. Ludwig, D., J.D., Holling, C.: Qualitative analysis of insect outbreak systems: The spruce budworm and forest. J. Anim. Ecol. **47**, 315–332 (1978)
25. Avlonitis, M. Zaiser, M.A.E.C.: Nucleation and non-linear strain localization during cyclic plastic deformation. J. Mech. Behav. Mater. **18**, 69–79 (2007)