A Quasi-species Model for the Propagation and Containment of Polymorphic Worms

Bradley Stephenson *Member, IEEE* and Biplab Sikdar *Member, IEEE*

Abstract—Polymorphic computer worms are characterized by their ability to change their byte sequence as they replicate and propagate, thereby aiming to thwart intrusion detection systems (IDSes). In this letter, we propose a model based on coevolution of biological quasi-species to characterize the propagation of polymorphic worms and the effect of IDSes on their dynamics. The model is used to derive the conditions required for the IDS to contain the worm. The model is validated using simulations.

Index Terms—Network security, computer virus and worms, modeling techniques

1 Introduction

Polymorphic techniques, which allow a worm to change its byte sequence with every instance, are increasingly being used to disguise worm payloads and attempt to bypass both signature and anomaly based IDSes. The objective of this letter is to develop a model for the propagation of polymorphic worms in the presence of a dynamic IDS. The model is then used to obtain: **(1)** the necessary conditions for the IDS to contain the spread of the worm and **(2)** the conditions governing the growth of various strains of the worm.

Understanding polymorphic worms remains a difficult and largely open problem. Existing papers on polymorphic worms either focus on developing mechanisms to detect them [1], [2], [3], [4], [5], [6], [7], [8] or study techniques they may use to evade the IDS [9], [10], [11], and not on modeling issues. On the other hand, papers that focus on developing propagation models for worms and other malware in the Internet such as [12], [13], [14] do not address polymorphic worms. Intrusion detection systems and their requirements have also been extensively studied (see [15], [16], [17], [18], [19], [20], [21], [22] and the references therein). Again, these either specifically focus on single strain worms and viruses or do not consider the coevolution of the worm and the IDS.

This letter fills a void in this area by developing an analytic framework for modeling and evaluating the dynamics of polymorphic worms. Our model is based on biological models for the coevolution of viral quasi-species and their interaction with the immune system [23], [24]. The morphing of code in polymorphic worms is analogous to the modifications in the genetic material of biological organisms in successive generations and this analogy was alluded to in [25]. The ability of the evolved organisms to survive depends on the ability of the immune system of the host to detect the new pathogen strains, analogous to the dependence of the survivability of new strains of the polymorphic worm on the effectiveness of the IDS. The evolution of the polymorphic worm's dynamics is modeled by a set of differential equations governing the co-evolutions of the quasi-species represented by the code sequences generated by the polymorphic worms, and the fitness landscape representing the capabilities of the IDS. We use these equations to evaluate the conditions required for the IDS to contain the worm. The observations from the model are validated using simulations.

The applicability of the model presented in this paper is limited to polymorphic worms. The model is not applicable to other possible and in some cases more effective ways to thwart IDSes such as metamorphic worms [1], [26], [27] and red herring [4] or allergy attacks [28]. The goal here is not to investigate the numerous ways in which a worm may try to confuse or overwhelm an IDS but rather to focus on the specific problem of modeling the population of polymorphic worms. Finally, some assumptions are made in this letter for analytic tractability, which while not always true, do not diminish the value of the insights gained from the model.

The rest of the letter is organized as follows. In Section 2 we present and discuss the assumptions made in our model. Section 3 presents our model and the results from the model are compared against simulations in Section 4. Conclusions are presented in Section 5.

2 Model Preliminaries and Assumptions

In this section we discuss the basic assumptions made in this letter. A discussion of polymorphism as it relates to

- *B. Stephenson now works at the MITRE Corporation, McLean, VA USA. The work was done while Brad Stephenson was at Rensselaer Polytechnic Institute, Troy, NY, USA. E-mail:stephenson@mitre.org*
- *B. Sikdar is with the Department of Electrical, Computer and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, USA. E-mail:sikdab@rpi.edu*

Manuscript received January 21, 2008; revised September 18, 2008. This work supported in part by NSF grant 0347623.

worms and our model can be found in [29]. Each copy of the worm is assumed to consist of an arbitrary (but fixed) number of strings or sequences. In this letter we refer to each worm with a different code sequence as a *strain*. In each generation the worm mutates some of the sequences to create new strains. We assume that the i^{th} sequence mutates independently with probability ϵ_i and its mutated sequences are chosen from an alphabet of size S_i. Each worm copy replicates at a rate of β.

An IDS system is assumed to be present in the network. We assume that the IDS has no knowledge of the worm initially but, depending on its capability, is able to detect some or all variations of the worm after a specific period of time. The model presented in this paper is not dependent on the exact techniques used by the IDS to detect the worms.

2.1 Discussion on the Assumptions

The objective of this letter is to give an intuition behind the propagation dynamics of polymorphic worms and some of the assumptions above have been made to keep the analysis tractable while avoiding an overwhelming number of variables. We now discuss these assumptions and their implications.

Our model assumes that in each successive replication, each byte sequence mutates independently. The independence in the mutations also means that they are harder to detect since there are no correlations that may be exploited.

The rate at which new infection attempts are made by real life worms depends on the scanning mechanism used and in certain scenarios, the replication rate decreases with time. We assume a constant replication rate representing the worst case scenario, leading to exponential growth in the worm population. This is consistent with the worm growth, detection and containment for the early stage of a worm and the model is accurate in these scenarios.

Another concern is the placement of the IDS system. In reality, it is impractical to expect each node to be equipped with an IDS and the effect of this can be captured to a certain extent by decreasing the detection rate of the IDS as the prevalence of IDS decreases. The model would however tend to underestimate the worm population since it assumes that all nodes infected by a known worm strain are detected.

3 Dynamics of Polymorphic Worms

In this section we develop our model for the evolution and spreading related dynamics of polymorphic worms.

3.1 Polymorphic Worm Propagation Model

Consider a worm composed of n strings or sequences. Let the strength or the total number of copies of strain k generated up until time t be denoted by $y_k(t)$. The time evolution of $y_k(t)$ is characterized by the following equation

$$\frac{dy_k(t)}{dt} = \sum_l \beta W_{l,k} A(y_l(t)) y_l(t) \tag{1}$$

where $W_{l,k}$ denotes the probability of a worm strain of type l morphing to a strain of type k in the next generation. $A(y_l(k))$ denotes the fitness function of strain l and accounts for the likelihood that the IDS is able detect and prevent the propagation of strain l. The summation above is carried out over all possible worm strains. Assuming each sequence to be of length b bits, we have $(2^b)^n$ possible worm strains. For example, even if we consider just 4 byte-long sequences characterizing a strain, we have a total of 2^{32} possible strain sequences. Thus considering each strain individually leads to an explosion in the state space and is impractical.

To make the model tractable, we group all strains according to their Hamming distance (HD) (i.e. the number of sequences in which the two strains differ) from a master strain (the master strain is the one which starts out with the highest strength and in the case of identical initial conditions, it may be chosen arbitrarily). Denoting the master strain by y_0, the l^{th} group is defined as

$$w_l = \sum_{y_k \in \{y_k | HD(y_k, y_0) = l\}} y_k \tag{2}$$

and its fitness function is defined by $A(l)$. This reduces the problem from $(2^b)^n$ dimensions to $n+1$ dimensions. We now derive the equations governing the time evolution of $w_l(t)$.

Claim 1: The time evolution of the strain group with Hamming distance l from the master strain is approximated by

$$\frac{dw_l(t)}{dt} = \sum_{l'=0}^{l} P_m(n,l,l') \beta A(l') w_{l'}(t) \tag{3}$$

where

$$P_m(n,l,l') = \sum_{j_1=1}^{n-l+1} \sum_{j_2=j_1+1}^{n-l+2} \cdots \sum_{j_{l-l'}=j_{l-l'-1}+1}^{n-l'} \frac{\epsilon_{j_1}\epsilon_{j_2}\cdots\epsilon_{j_{l-l'}} \prod_{i=1}^{n}(1-\epsilon_i)}{(1-\epsilon_{j_1})(1-\epsilon_{j_2})\cdots(1-\epsilon_{j_{l-l'}})}$$

is the probability of a worm from strain group l' mutating to strain group l and $P_m(n,l,l') = \prod_{i=1}^{n}(1-\epsilon_i)$ if $l - l' = 0$. In the case $\epsilon_i = \epsilon$, $\forall i$, the above expression reduces to $P_m(n,l,l') = \binom{n-l'}{l-l'} \epsilon^{l-l'} (1-\epsilon)^{n-(l-l')}$.

Proof: The proof is given in Appendix 1. □

In Equation (3), a key parameter is the fitness function $A(l')$ corresponding to each group. In the absence of any defense mechanism, the fitness function for each group will be the same since all of them are equally likely to propagate without detection. We thus consider a scenario where initially all the strains have an identical fitness function (we introduce the effect of the IDS later in this section)

$$A(y_l) = \eta, \quad \forall l \quad \Rightarrow \quad A(w_l) = \eta \quad \forall l \tag{4}$$

In order to determine the maximum allowable response time of the IDS, we now obtain the strengths of arbitrary members of different strain groups. In the following, we assume that each strain *group* has the same initial strengths, i.e.

$$w_l(0) = w_0(0) \qquad \forall l \tag{5}$$

The above expression implies that the initial strength of the an arbitrary member of the strain group with Hamming distance 1 will have lower initial strength than an arbitrary member of the strain group with Hamming distance 0. This is because there are $\sum_{i=1}^{n}(S_i-1)$ members in the group with Hamming distance 1 as compared to only one member in the latter group and the initial strengths of the groups are identical. A similar argument applies to other groups. This is in line with most real life attacks that are initiated by only a few specimens and then spread using other variants or strains. Note that by making the initial strength of strain group with Hamming distance 1 $\sum_{i=1}^{n}(S_i-1)$ times higher than that of the strain group with Hamming distance 0 (and so on for other groups), we can accommodate the case where all strains have the same initial strength.

Claim 2: The strength of an arbitrary member of the 0^{th}, 1^{th} and n^{th} strain group, represented by w_0^a, w_1^a and w_n^a respectively, the total worm strength w and the number of different strains existing in the network, N, are

$$w_0^a(t) = w_0(0)e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t} \tag{6}$$

$$w_1^a(t) = w_0(0)\frac{e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t}}{\sum_{k=1}^{n}(S_k-1)}\left[1+\beta\eta t\sum_{j=1}^{n}\epsilon_j\prod_{l=1}^{n}\frac{1-\epsilon_l}{1-\epsilon_j}\right] \tag{7}$$

$$w_n^a(t) = w_0(0)\frac{e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t}}{\prod_{k=1}^{n}(S_k-1)} \tag{8}$$

$$w(t) = w_0(0)(n+1)e^{\beta\eta t} \tag{9}$$

$$N(t) = w_0(0)(n+1)\left[1-\prod_{i=1}^{n}(1-\epsilon_i)\right]\left[e^{\beta\eta t}-1\right]+N(0) \tag{10}$$

where $w_0(0) = y_0(0)$ is the initial strength of the master strain $w_0(t)$ and N(0) is the initial number of strains in the network.

Proof: We consider each strain group separately and solve Equation (3) to obtain the expressions above.

Strain group 0: Note that there is only one strain (the master strain) which belongs to the 0^{th} strain group and thus $w_0^a(t) = w_0(t)$. From Equation (3), substituting $l = 0$, we have

$$\begin{aligned}\frac{dw_0^a(t)}{dt} &= \frac{dw_0(t)}{dt} = A(w_0)\prod_{i=1}^{n}(1-\epsilon_i)\beta w_0(t)\\ &= \eta\prod_{i=1}^{n}(1-\epsilon_i)\beta w_0(t)\end{aligned} \tag{11}$$

Solving the ordinary differential equation above, we obtain

$$w_0^a(t) = w_0(0)e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t} \tag{12}$$

where $w_0(0) = w_0^a(0) = y_0(0)$, the initial strength of the master strain.

Strain group 1: With each worm strain consisting of n sequences and an alphabet of size S_k for sequence k, there are $\sum_{k=1}^{n}(S_k-1)$ possible strains which have a Hamming distance of 1 from the master strain and thus form group 1. Thus the dynamics of the group $w_1(t)$ is $\sum_{k=1}^{n}(S_k-1)$ times faster than an arbitrary strain $w_1^a(t)$ in the group. Substituting $l = 1$ in Equation (3) we then have

$$\begin{aligned}\frac{dw_1^a(t)}{dt} &= \frac{1}{\sum_{k=1}^{n}(S_k-1)}\frac{dw_1(t)}{dt} = \sum_{l'=0}^{1}\frac{P_m(n,1,l')\beta A(l')}{\sum_{k=1}^{n}(S_k-1)}w_{l'}(t)\\ &= \frac{\beta\eta\prod_{l=1}^{n}(1-\epsilon_l)}{\sum_{k=1}^{n}(S_k-1)}\left[\sum_{j=1}^{n}\frac{\epsilon_j}{1-\epsilon_j}e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t}w_0(0)+w_1(t)\right]\end{aligned}$$

Solving the differential equation above and using $w_1(0) = w_0(0)$, we obtain

$$w_1^a(t) = w_0(0)\frac{e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t}}{\sum_{k=1}^{n}(S_k-1)}\left[1+\beta\eta t\sum_{j=1}^{n}\epsilon_j\prod_{l=1}^{n}\frac{1-\epsilon_l}{1-\epsilon_j}\right] \tag{13}$$

Strain group n: Consider an arbitrary member of strain group n, w_n^a. Denote by $\Omega_m^{i,j}$ the set of sequences of the j^{th} strain in group i, w_i^j, that are identical with the sequences of w_n^a. Increase in the strength of w_n^a results from its own growth as well as the mutations from members of all other groups and other members of its own group. These contributions are

$$\begin{aligned}\frac{dw_n^a(t)}{dt} &= A(w_n)\beta\prod_{l=1}^{n}(1-\epsilon_l)w_n^a(t)+\\ &\sum_{i=0}^{n}\sum_{w_i^j\in\{w_i,w_n^j\neq w_n^a\}}A(w_i)\beta\prod_{k\notin\Omega_m^{i,j}}\frac{\epsilon_k}{S_k-1}\prod_{l\in\Omega_m^{i,j}}(1-\epsilon_l)w_i^j(t)\end{aligned}$$

In the expression above, a mutation from any strain j of group i, $1 \le i \le n$ to the strain w_n^a occurs when: (1) each sequence k in w_i^j that is not in $\Omega_m^{i,j}$ mutates to the corresponding sequence in w_n^a, each of which happens with probability $\frac{\epsilon_k}{S_k-1}$ and (2) each of the remaining sequences $l \in \Omega_m^{i,j}$ do not mutate, the probability of which is $1-\epsilon_l$. Also, members of strain w_n^a continue to replicate their own if no mutation occurs, i.e. with probability $\prod_{j=1}^{n}(1-\epsilon_j)$. Note that in the expression above, the second term has a product term of (S_k-1) in the denominator. For even small alphabet sizes and number of sequences, the contribution of the second term becomes quite small and we can thus write

$$\frac{dw_n^a(t)}{dt} \approx A(w_n)\beta\prod_{i=1}^{n}(1-\epsilon_i)w_n^a(t) = \beta\eta\prod_{i=1}^{n}(1-\epsilon_i)w_n^a(t)$$

Solving the differential equation above gives

$$w_n^a(t) = w_n^a(0)e^{\beta\eta\prod_{i=1}^{n}(1-\epsilon_i)t} = w_0(0)\frac{e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t}}{\prod_{k=1}^{n}(S_k-1)} \tag{14}$$

Overall worm population: The overall worm population constitutes of the populations of each worm strain or strain group. The rate of change of the overall worm population is given by

$$\begin{aligned}\frac{dw(t)}{dt} &= \sum_{l=0}^{n}\frac{dw_l(t)}{dt} = \sum_{l=0}^{n}\sum_{y_k\in\{y_k|HD(y_k,y_0)=l\}}\frac{dy_k(t)}{dt} \\ &= \sum_{l=0}^{n}\sum_{y_k\in\{y_k|HD(y_k,y_0)=l\}}\sum_{i}\beta\eta W_{i,k}y_i(t) \quad (15)\\ &= \beta\eta\sum_i\sum_j W_{i,j}y_i(t) \quad (16)\\ &= \beta\eta\sum_i y_i(t) = \beta\eta w(t) \quad (17)\end{aligned}$$

where the third summation in Eqn. (15), and the two summations in Eqn. (16) are carried out over all strains (y_k). Also, in Eqn. (17) we have used the fact that $\sum_j W_{i,j} = 1$, $\forall i$. Solving the differential equation above, we get

$$w(t) = w_0(0)(n+1)e^{\beta\eta t} \quad (18)$$

where we have used the fact that the initial worm population is $(n+1)w_0(0)$.

Number of strains: At each replication attempt, the new worm is different from the one at the infecting node with probability $1-\prod_{i=1}^{n}(1-\epsilon_i)$. While the new worm may be the same as any of the existing worms, the likelihood of this event is small because (i) the probability of down-mutations is very small as shown in the proof of Claim 1, (ii) given that a worm strain at a Hamming distance of l exists in the network, the probability of up-mutating is $\prod^{l}\frac{\epsilon_i}{S_i-1}\prod^{n-l}(1-\epsilon_j)$ (fairly small) and (iii) most of the strains with higher Hamming distances from the master strain are unpopulated (for example, with $S = 256$ there are over 4 billion strains with a Hamming distance of 4, most of which are unpopulated). Thus to a very good approximation it may be assumed that each mutation leads to a new strain in the time scales of our interest. Since from Eqn. (17) each worm replicates with rate $\beta\eta$, we have

$$\frac{dN(t)}{dt} = \left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)\beta\eta w(t) \quad (19)$$

Solving Eqn. (17) and (19) simultaneously we have

$$N(t) = w_0(0)(n+1)\left[1-\prod_{i=1}^{n}(1-\epsilon_i)\right]\left[e^{\beta\eta t}-1\right]+N(0) \quad (20)$$

For the special case where $w_0(0) = 1$, we have $N(0) = n+1$. This completes the proof of Claim 2. □

3.2 Maximum Allowable IDS Response Time

In this subsection we assume that the time interval between the first infection and the first detection by the IDS is τ and then τ_{ids} seconds elapse between the detection of successive instances of the worm. We now obtain the minimum rate at which the IDS must detect new strains in order to contain the growth of the worm population.

3.2.1 A Simple Bound

Let α be the rate at which new strains must be detected in order to contain the worm. The approach for deriving α is to characterize the required detection rate as a fraction $\frac{1}{k}$ of the number of worm strains existing in the network at the time of first detection ($N(\tau)$) so that the worm population is a decreasing function of time (i.e., α is expressed in terms of k and the inital conditions and the bounds are then derived for k). One unit of time after τ, in the absence of any new worms being generated, the number of remaining strains is then

$$N(\tau) - \frac{N(\tau)}{k} = N(\tau)\left(1-\frac{1}{k}\right) \quad (21)$$

It is more likely that worm strains with greater strength would be detected before strains with lower strengths. Then, the number of remaining worms after one unit time's detection would be at most $w(\tau)(1-\frac{1}{k})$. Each of these worms (or infected nodes) infects other nodes at rate $\beta\eta$ and each infection results in a new strain with probability $1-\prod_{i=1}^{n}(1-\epsilon_i)$. Using Eqn. (17), the number of new worms generated in an unit of time after the first detection is then

$$\Delta w(\tau) \triangleq w(\tau+1)-w(\tau) = \left(1-\frac{1}{k}\right)w(\tau)\left(e^{\beta\eta}-1\right) \quad (22)$$

The number of worm strains after one unit of time is then at most

$$N(\tau)\left(1-\frac{1}{k}\right) + \left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)\Delta w(\tau) \quad (23)$$

and to ensure that the worm growth is contained, this number should be less than $N(\tau)$, i.e.,

$$N(\tau)\left(1-\frac{1}{k}\right)+\left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)w(t)\left(e^{\beta\eta}-1\right)\left(1-\frac{1}{k}\right) < N(\tau)$$

Solving for k we then have

$$k < 1 + \frac{N(\tau)}{(1-\prod_{i=1}^{n}(1-\epsilon_i))w(\tau)\left(e^{\beta\eta}-1\right)} \quad (24)$$

Since $N(\tau+1) < N(\tau)$ with this choice of k, continuing to detect $\frac{N(\tau)}{k}$ strains per unit time monotonically keeps decreasing the number of strains present in the network. Thus it suffices to have

$$\alpha > \frac{N(\tau)}{k} \quad (25)$$

to contain the worm and $\tau_{ids}^{1} < \frac{1}{\alpha}$.

3.2.2 Containment Time Dependent Signature Generation

In the previous subsection, we obtained an expression for the strain detection rate required to ensure that the worm population is a decreasing function of time. With finite number of nodes in a network, a very slow detection rate will also eventually succeed in detecting all infected nodes but after all nodes in the network have been infected. We now consider the case where we need to detect new strains fast enough so that all existing worm strains are detected within a specified amount of time. With the time at which the first worm strain is detected denoted by τ, let $\tau+T$ be the time at which all worm strains are required to be detected.

From Eqn. (9) and (10), the number of infected nodes and the number of worm strains at time τ are given by

$$w(\tau) = w_0(0)(n+1)e^{\beta\eta\tau} \tag{26}$$

$$N(\tau) = w_0(0)(n+1)(1-\textstyle\prod_{i=1}^{n}(1-\epsilon_i))[e^{\beta\eta\tau}-1]+N(0) \tag{27}$$

Since α strains are detected in an unit of time, the rate of change of the number of strains is

$$\frac{dN(t)}{dt} = \left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)\beta\eta w(t) - \alpha \tag{28}$$

Since the strains with higher strength are detected first, the strength of a detected strain is at least $\frac{w(t)}{N(t)}$. The rate of change in the worm population is then

$$\frac{dw(t)}{dt} = \beta\eta w(t) - \alpha\frac{w(t)}{N(t)} \tag{29}$$

Solving Eqn. (28) and (29) simultaneously, we obtain

$$w(T) = Ae^{\beta\eta T}\frac{\alpha w(\tau)}{\beta\eta\left[N(\tau)-(1-\prod_{i=1}^{n}(1-\epsilon_i))w(\tau)\right]} \tag{30}$$

$$N(T) = \frac{\alpha A}{\beta\eta e^{-\beta\eta T}}\left[e^{-\beta\eta T}+\frac{(1-\prod_{j=1}^{n}(1-\epsilon_j))w(\tau)}{N(\tau)-(1-\prod_{i=1}^{n}(1-\epsilon_i))w(\tau)}\right] \tag{31}$$

where

$$\begin{aligned} A &= \ln\left(\frac{\left(e^{-\beta\eta T}+\frac{w(\tau)(1-\prod_{i=1}^{n}(1-\epsilon_i))}{N(\tau)-(1-\prod_{j=1}^{n}(1-\epsilon_j))w(\tau)}\right)}{N(\tau)[N(\tau)-(1-\prod_{k=1}^{n}(1-\epsilon_k))w(\tau)]^{-1}}\right) \\ &\quad +\left(\frac{\alpha+\beta\eta N(\tau)-(1-\prod_{l=1}^{n}(1-\epsilon_l))\beta\eta w(\tau)}{\alpha}\right)-1 \end{aligned}$$

To obtain the desired detection rate α that will detect all existing strains within time T, we can equate either Eqn. (30) or Eqn. (31) to zero and solve for α. This solution gives us

$$\alpha = \frac{\beta\eta N(\tau)-\beta\eta(1-\prod_{k=1}^{n}(1-\epsilon_k))w(\tau)}{\ln\left(\frac{N(\tau)}{e^{-\beta\eta T}\left(N(\tau)-(1-\prod_{i=1}^{n}(1-\epsilon_i))w(\tau)\right)+(1-\prod_{j=1}^{n}(1-\epsilon_j))w(\tau)}\right)} \tag{32}$$

and thus $\tau_{ids}^2 < \frac{1}{\alpha}$. At lower mutation rates, the equation above may overestimate the required rate at which new strains must be detected. This is because the derivation assumes each detected strain has a strength of $\frac{w(t)}{N(t)}$ while in reality the dominant strain may have higher numbers. To reduce the resulting error, we combine Eqns. (25) and (32) to give

$$\tau_{ids} = \min\{\tau_{ids}^1, \tau_{ids}^2\} \tag{33}$$

3.3 Non Fixed Rate Detection Mechanisms

In many practical IDSes, the time between successive strain detections may be a function of time or dependent on the number of stains seen by the IDSes so far. We now extend our models for these scenarios.

We first consider the case where the rate at which new strains are detected is a polynomial function γt^ν of the time t that has elapsed after the first detection (τ). Here γ is an arbitrary positive constant included for generality. In this case, the rate of change in the number of strains and the worm population in the network are given by

$$\frac{dN(t)}{dt} = \left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)\beta\eta w(t) - \gamma t^\nu \tag{34}$$

$$\frac{dw(t)}{dt} = \beta\eta w(t) - \gamma t^\nu\frac{w(t)}{N(t)} \tag{35}$$

with the initial conditions given in Eqn. (26) and (27). While no closed form expression for the simultaneous solution of Eqn. (34) and (35) exists, they may be solved numerically to obtain the ν required for the worm population to die out within a given period.

Next we consider the case where the rate of strain detection depends on the number of strains that have appeared in the network so far. Let $x(t)$ be the count of the number of strains seen in the network till time t. After the first detection at time τ, the rate of new detections is given by $\mu x(t)$. The rate of change in the total and existing number of strains, and the worm population in the network are given by

$$\frac{dx(t)}{dt} = \left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)\beta\eta w(t) \tag{36}$$

$$\frac{dN(t)}{dt} = \left(1-\prod_{i=1}^{n}(1-\epsilon_i)\right)\beta\eta w(t) - \mu x(t) \tag{37}$$

$$\frac{dw(t)}{dt} = \beta\eta w(t) - \mu x(t)\frac{w(t)}{N(t)} \tag{38}$$

with $x(\tau) = N(\tau)$ and the other two initial conditions given in Eqn. (26) and (27). Again, no closed form expression for the simultaneous solution of Eqn. (37), (37) and (38) exists. They may be solved numerically to obtain the μ required for the worm population to die out within a given period.

3.4 Further Analysis: Dominant Group Populations

We now consider the dominance of one strain group over the other and evaluate the interaction between the polymorphic worm and the IDS in detail. Once the IDS detects the strain with the highest strength, it applies a large kill rate δ to that specific worm strain. Until the IDS is capable of detecting the other strains of the worm, other worm strains will now have a higher growth rate as compared to the earlier dominant strain. The worm adapts to this change in the fitness landscape and the strain with the next highest strength now becomes the dominant strain. The IDS system now tries to adapt to this new dominant strain. Through the iteration of the steps above, the worm scours through the sample space of strains and the IDS system follows on its heels.

Once the IDS detects the master strain, strains belonging to strain group 1 have the next highest strength while those belonging to strain group n have the lowest, as can be observed from Eqns. (6), (7) and (8). The continuation of this dominance depends on the timescale $\tau = \tau_{ids} + \tau_w$, i.e. on the speed with which the IDS detects new strains (τ_{ids}) and how fast the worm adapts to the changing fitness landscape (τ_w). In the following, we investigate the conditions required for this dominance, assuming new strains are detected at a constant rate.

Let $t = 0$ be the instant when the fitness landscape shifts and an arbitrary strain from the 1^{st} strain group becomes dominant. Using Eqn. (7) the normalized growth of this strain over a period τ is then given by

$$\frac{w_1^a(\tau)}{w_1^a(0)} = \frac{e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta t}}{\sum_{k=1}^{n}(S_k-1)}\left[1+\beta\eta t\sum_{j=1}^{n}\epsilon_j\prod_{l=1}^{n}\frac{1-\epsilon_l}{1-\epsilon_j}\right] \quad (39)$$

The strain w_1^a is currently the fittest. But if another strain far away from the fitness peak is able to surpass its population in the interval τ, then the currently dominant strain will lose its dominance. With the current dominant strain being from strain group 1 and the strain group 0 having already been detected, we turn to an arbitrary member of the strain group n, w_n^a, since it has the largest Hamming distance from the master sequence. Using Equation (8), its normalized growth rate is then given by

$$\frac{w_n^a(\tau)}{w_n^a(0)} = e^{\beta\eta\prod_{i=1}^{n}(1-\epsilon_i)\tau} \quad (40)$$

The ratio of these growth rates is then

$$\kappa = \frac{\frac{w_1^a(\tau)}{w_1^a(0)}}{\frac{w_n^a(\tau)}{w_n^a(0)}} = \frac{1+\beta\eta\tau\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}}{\sum_{k=1}^{n}(S_k-1)} \quad (41)$$

The member of strain group 1 will lose its dominance if $\kappa < 1$ and dominates only when $\kappa \geq 1$. To evaluate κ we next obtain an expression for τ. To estimate the timescale for the shift in the worm's fitness landscape, τ_w, we first iterate the propagation model for a full cycle of length τ starting at $t = 0$. The switch in the dominant strain is made at $t = \tau$ when the IDS starts applying the decay rate of δ on the previous dominant strain. Now, the populations of the old and new dominant strains at the end of τ are given by $w_0^a(\tau)$ and $w_1^a(\tau)$ in Equations (6) and (7) respectively. In the subsequent interval τ_w, the growth rates of the old and new dominant strains are $e^{\prod_{i=1}^{n}(1-\epsilon_i)\eta\beta-\delta}$ and $e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta}$ respectively. Equating the populations of the old and new dominant strains at τ_w, we obtain

$$\begin{aligned}
& e^{\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta\tau_w} w_1^a(\tau) = e^{\prod_{i=1}^{n}(1-\epsilon_i)(\beta\eta-\delta)\tau_w} w_0^a(\tau) \\
\Rightarrow\ & e^{\prod_{l=1}^{n}(1-\epsilon_l)\beta\eta\tau_w} e^{\prod_{m=1}^{n}(1-\epsilon_m)\beta\eta\tau\frac{1+\beta\eta\tau\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}}{\sum_{k=1}^{n}(S_k-1)}} \\
& \qquad = e^{(\prod_{i=1}^{n}(1-\epsilon_i)\beta\eta-\delta)\tau_w} e^{\prod_{j=1}^{n}(1-\epsilon_j)\beta\sigma\tau} \\
\Rightarrow\ & \tau_w = -\frac{1}{\delta}\ln\left(\frac{1+\beta\eta\tau\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}}{\sum_{k=1}^{n}(S_k-1)}\right) \quad (42)
\end{aligned}$$

Using Equation (42), we can write τ as

$$\begin{aligned}
\tau = \tau_w + \tau_{ids} &= -\frac{1}{\delta}\ln\left(\frac{1+\beta\eta\tau\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}}{\sum_{k=1}^{n}(S_k-1)}\right)+\tau_{ids} \\
&= \frac{1}{\delta}\text{LamW}(x) - \frac{1}{\beta\eta\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}} \quad (43)
\end{aligned}$$

where x is given by

$$x = \frac{\delta\sum_{k=1}^{n}(S_k-1)}{\beta\eta\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}} e^{\frac{\delta\left[1+n\beta\eta\tau_{ids}\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}\right]}{\beta\eta\sum_{j=1}^{n}\epsilon_j\prod_{i=1}^{n}\frac{1-\epsilon_i}{1-\epsilon_j}}} \quad (44)$$

and $\text{LamW}(\cdot)$ is the Lambert W function, i.e., a function which satisfies

$$\text{LamW}(y)e^{\text{LamW}(y)} = y \quad (45)$$

3.4.1 Worm Mutation Rates

For the special case of $\epsilon_i = \epsilon, \forall i$, we now further analyze the quasi-species model to determine the mutation rate of the polymorphic worm that maximizes the likelihood of worms of strain group 1 dominating those of group n. With the ratio κ in Equation (41) governing the dominance of strain group 1, obtaining this mutation rate requires solving for $\frac{\partial\kappa}{\partial\epsilon} = 0$, which can be written as

$$\begin{aligned}
\frac{\partial\kappa}{\partial\epsilon} &= \frac{\partial}{\partial\epsilon}\frac{1+n\beta\eta\epsilon(1-\epsilon)^{n-1}\tau}{n(S-1)} \\
&= \frac{\partial}{\partial\epsilon}\frac{\beta\eta\epsilon(1-\epsilon)^{n-1}\tau}{S-1}
\end{aligned}$$

Substituting the value of τ from Equations (42) and (44) into the equation above, we have

$$0 = \frac{\partial}{\partial\epsilon}\frac{\beta\eta\epsilon(1-\epsilon)^{n-1}}{S-1}\left[\frac{1}{\delta}\text{LamW}(x) - \frac{1}{n\beta\eta\epsilon(1-\epsilon)^{n-1}}\right]$$

After some algebraic manipulations of the equation above we have the mutation rate ϵ_{opt} as the solution of the following equation for ϵ

$$\big[1+\text{LamW}(x)\big]x = \frac{\epsilon(1-\epsilon)}{n\epsilon-1} \quad (46)$$

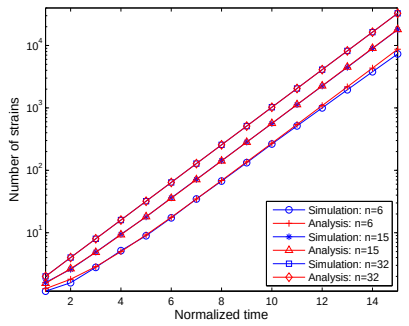

Fig. 1. The number of distinct strains in the network as a function of time.

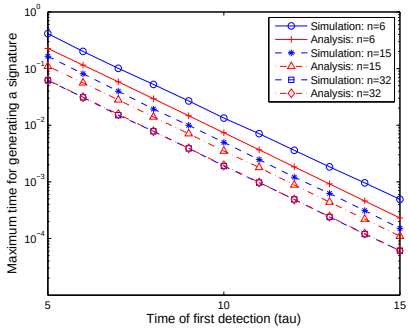

Fig. 2. The maximum allowable detection time with constant detection rate as a function of τ.

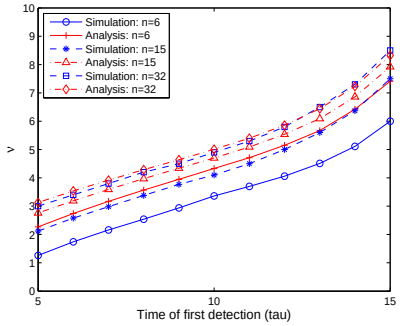

Fig. 3. The ν required for containment with polynomial detection rate as a function of τ.

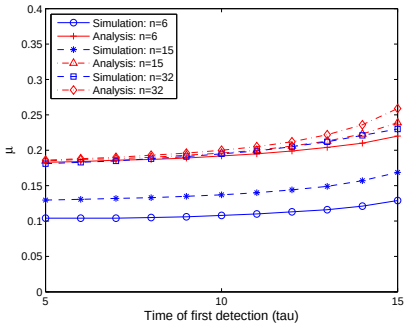

Fig. 4. The μ required for containment with proportional detection rate as a function of τ.

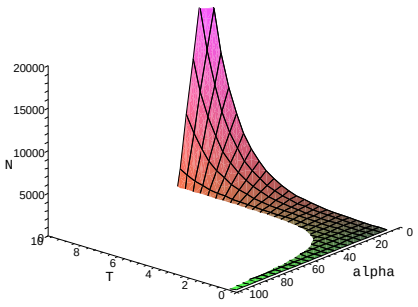

Fig. 5. The worm populating as a function of T and α for $\epsilon = 0.55$ (constant detection rate).

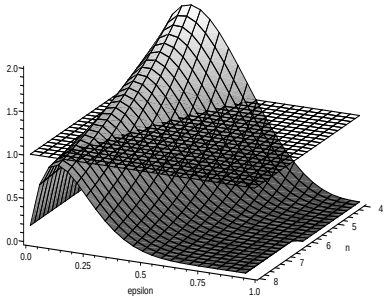

Fig. 6. κ versus ϵ and n. The parameters used are $\eta = 1.0$, $\beta = 100$, $\delta = 100$, $\tau_{ids} = 40$ and $S = 255$.

4 Simulation Results

To verify the models presented in the previous sections, in this section, we compare the analytical results with those from simulations. The simulator core was based on a random scanning engine provided to us by the authors of [30]. This simulator was used to generate the results in [30] and is based on permutation scanning of the address space. In permutation scanning, all worms share a common pseudo-random permutation of the IP address space and an infected machine starts scanning just after its location in the permutation. Permutation scanning prevents the same address from being scanned multiple times and the worm thus propagates faster. To implement the polymorphic part, we combined the worm generator of [30] with the `ADMutate` polymorphic engine [31]. Thus the selection of the nodes to be infected was made according to the permutation scanning of [30] and the worm code that infects the node was generated according to the `ADMutate` engine. After each detection step, the worm strain with the highest strength was detected by the simulated IDS and these worms were prevented from propagating further in the network. Our simulator takes the following inputs: n, τ_{ids}, β and the number of initially infected nodes and uses $\eta = 1$.

For the results presented in this section, we have normalized a unit of time to the time required for an infected node to attempt infecting another node. Equivalently, $\beta = 1$ in our simulations. Results for other values of β are simply scaled versions of the results presented here. Also, a single node was assumed to be infected initially. Results are presented for three values of the size of the worm content scanned by the IDS for detection purposes: 6, 15 and 32 bytes. For the 6 byte case, two bytes had ϵ and S of 0.03 and 16 respectively (denoted as $2\times[0.03, 16]$) while the remaining four had corresponding values of 0.06 and 255 ($4 \times [0.06, 255]$). For the 15 byte case we had: $4\times[0.03, 16]$ and $11\times[0.06, 255]$ and for the 32 byte case: $6 \times [0.03, 16]$, $2 \times [0.99, 55]$, $4 \times [0.80, 255]$, $2\times[0.94, 255]$ and $18\times[0.06, 255]$. The alphabet size of 16 corresponds to the least significant nibble of the return address that is cycled by the `ADMutate` engine, the alphabet size of 55 corresponds to the NOPs and that of 255 bytes corresponds to other content in the worm payload. The mutation rates and alphabet sizes were empirically observed though multiple (2000) runs of the `ADMutate` engine. Each simulation was repeated with 100 different seeds and the average values are reported. The 95% confidence interval for all results was within 10% of the mean.

In Figure 1 we compare the simulation and analytic

results for the number of strains in the network as a function of time. In Figure 2 we plot the maximum allowable time for detecting a new strain for containment in the case of constant detection rates. The match between the simulation and analytic results improves as n and ϵ increase and we note an almost exact match for the 32 byte case. The difference at lower mutation rates is because in Eqn. (28) the change in the worm population at each detection is assumed to be $\frac{w(t)}{N(t)}$, while in the simulations, the strain with the highest strength is detected. Thus the worm population in the simulations falls faster and higher detection times are sufficient to control the worm population. At higher mutation rates each mutation is more likely to lead to a new strain and thus the populations of all strains are likely to be closer, and in this case the analytic model gives very accurate results. Similar trends are observed in Figures 3 and 4 which show the required value of ν and μ for worm containment in the case of polynomial and proportional detection rates.

We next consider the analytic results for the IDS with constant detection rates to gain further insight into the dynamics of the worm. In Figure 5 we show the worm population $N(t)$ as a function of α and T, the time from the first detection, for $n = 84$, $\epsilon = 0.55$ and $\tau = 5$. For lower values of T, the α required to contain the worm increases and the asymptote in the figure also shows the minimum α value required to contain the worm. Finally, in Figure 6 we plot κ as a function of ϵ and n. We also plot the plane $\kappa = 1$ to show the dominance criterion. We note that the dominance of strain 1 peaks at values of ϵ where the likelihood of zero or single mutations is maximized since this leads to their fastest growth. We also note that as n increases, the value of κ decreases. This is because as the signature length increases, the IDS becomes better at detecting the worm strains. Note that for $n = 8$, there is no portion of the surface which meets the dominance criterion since now each new infection is likely to have more than one mutations, reducing the growth rate of members of strain group 1.

5 Conclusions

In this letter we presented a framework based on co-evolution of quasi-species to model the dynamics of polymorphic worms and their interaction with an IDS. The model provides a theoretical basis to explain polymorphic worm outbreaks and the limitations they put on the IDS and thereby aid the development of defense strategies which can respond effectively to such outbreaks. The model is used to obtain the conditions that govern the growth, containment and dominance of worm strains.

Appendix

We now present the proof for Claim 1.

Proof: Mutations into group l may occur in two possible ways: (1) up-mutations from groups with lower Hamming distances and (2) down-mutations from groups with larger Hamming distances. Consider the up-mutation case first with mutations from group l' to group l with $l' \leq l$. There are three possibilities for the up-mutation:

i. $l - l'$ of the $n - l'$ sequences which are identical with the master sequence mutate and all other sequences stay the same. This case, C1, occurs with probability

$$P[\text{C1}] = P_m(n, l, l') \tag{47}$$

ii. i, $0 < i \leq \min\{l', n - l\}$, of the already mutated sequences mutate back to the master strain and there are mutations in $l - l' + i$ of the $n - l'$ non-mutated sequences. Let $\Omega_{l'}$ be the set of sequences of the worm that have already mutated ($|\Omega_{l'}| = l'$) and $\Omega^c_{l'}$ be the rest of the sequences ($|\Omega^c_{l'}| = n - l'$). Also, let $\phi_1, \phi_2, \cdots, \phi_{l'}$ ($\psi_1, \psi_2, \cdots, \psi_{n-l'}$) be the elements of $\Omega_{l'}$ ($\Omega^c_{l'}$), i.e. the positions of the bytes that have mutated (not-mutated). Now, the probability that sequence k mutates and changes back to the corresponding sequence in the master strain is given by $\frac{\epsilon_k}{S_k - 1}$. Then the probability of this case, C2, is given by

$$P[\text{C2}] = \sum_{i=1}^{\min\{l', n-l\}} \left[\bigoplus_{b, l-l'+i}^{n-l'} \frac{\epsilon_{\psi_{b_1}} \epsilon_{\psi_{b_2}} \cdots \epsilon_{\psi_{b_{l-l'+i}}}}{(1-\epsilon_{\psi_{b_1}})(1-\epsilon_{\psi_{b_2}}) \cdots (1-\epsilon_{\psi_{b_{l-l'+i}}})} \right.$$
$$\left. \bigoplus_{a,i}^{l'} \frac{\epsilon_{\phi_{a_1}} \epsilon_{\phi_{a_2}} \cdots \epsilon_{\phi_{a_i}}}{(S_{\phi_{a_1}} - 1)(S_{\phi_{a_2}} - 1) \cdots (S_{\phi_{a_i}} - 1)} \frac{\prod_{k=1}(1 - \epsilon_k)}{(1-\epsilon_{\phi_{a_1}}) \cdots (1-\phi_{a_i})} \right]$$

where $\bigoplus_{a,A}^{B} = \sum_{a_1=1}^{B-A+1} \sum_{a_2=a_1+1}^{B-A+2} \cdots \sum_{a_A=a_{A-1}+1}^{B}$.

iii. Of the l' already mutated sequences, i mutate back to the corresponding sequences in the master strain, j ($j > 0$) mutate to other sequences, $l' - i - j$ stay the same with $i + j \leq l'$ and $0 < i \leq \min\{l', n - l\}$ and of the $n - l'$ non-mutated sequences, $l - l' + i$ sequences mutate and the remaining $n - l - i$ sequences stay the same. For a given i, let $\Omega^B_{l''}$ be the set of sequences that are not back-mutating ($|\Omega^B_{l''}| = l' - i$) and let $\varphi_1, \varphi_2, \cdots, \varphi_{l'-i}$ be the elements of $\Omega^B_{l'}$. The case C3 then occurs with probability

$$P[\text{C3}] = \sum_j \sum_i \left[\bigoplus_{a,i}^{l'} \frac{\epsilon_{\phi_{a_1}}(1-\epsilon_{\phi_{a_1}})^{-1}}{(S_{\phi_{a_1}} - 1)} \cdots \frac{\epsilon_{\phi_{a_i}}(1-\epsilon_{\phi_{a_i}})^{-1}}{(S_{\phi_{a_i}} - 1)} \right.$$
$$\bigoplus_{b,j}^{l'-i} \frac{\epsilon_{\varphi_{b_1}}(S_{\varphi_{b_1}} - 2)}{(S_{\varphi_{b_1}} - 1)} \cdots \frac{\epsilon_{\varphi_{b_j}}(S_{\varphi_{b_j}} - 2)}{(S_{\varphi_{b_j}} - 1)} \bigoplus_{c, l-l'+1}^{n-l'} \frac{\epsilon_{\psi_{c_1}}}{1 - \epsilon_{\psi c_1}} \cdots$$
$$\left. \frac{\epsilon_{\psi_{c_{l-l'+i}}}}{1 - \epsilon_{\psi_{c_{l-l'+i}}}} \frac{\prod_{k=1}^{n}(1-\epsilon_k)}{(1-\epsilon_{\varphi_{b_1}}) \cdots (1-\epsilon_{\varphi b_j})} \right]$$

where the summations over i and j are carried out over the region where $j > 0$, $i + j \leq l'$ and $0 < i \leq \min\{l', n - l\}$.

We now consider the down-mutations where strains with a higher Hamming distance l' back-mutate to generate strains with lower Hamming distance l ($l < l'$) from the master strain. Again, there are three possibilities:

i. $l'-l$ of the already mutated sequences mutate back to the corresponding sequences in the master strain while the remaining sequences stay the same. This case, C4, occurs with probability

$$P[\text{C4}] = \bigoplus_{a,l'-l}^{l'} \frac{\epsilon_{\phi_{a_1}}(1-\epsilon_{\phi_{a_1}})^{-1}}{(S_{\phi_{a_1}}-1)} \cdots \frac{\epsilon_{\phi_{a_{l'-l}}}(1-\epsilon_{\phi_{a_{l'-l}}})^{-1}}{(S_{\phi_{a_{l'-l}}}-1)} \prod_{k=1}^{n}(1-\epsilon_k)$$

ii. i of the already mutated sequences mutate back to the corresponding sequences in the master strain with $l'-l < i \leq \min\{l', n-l\}$ and $l-l'+i$ of the $n-l'$ non-mutated sequences mutate while the remaining sequences stay the same. The expression for the probability of this case, $P[\text{C5}]$, is the same as that for case C2 except that now the initial summation is carried out over $\sum_{i=l'-l+1}^{\min\{l',n-l\}}$.

iii. Of the l' already mutated sequences, i mutate back to the corresponding sequences in the master strain (where $l'-l < i \leq \min\{l', n-l\}$), j ($0 < j < i$ and $i+j \leq l'$) mutate to other sequences, $l'-i-j$ stay the same and of the $n-l'$ non-mutated sequences, $l-l'+i$ sequences mutate and the remaining $n-l-i$ sequences stay the same. The expression for the probability of this case, $P[\text{C6}]$, is the same as that for case C3, except that now the summations over i and j are carried out over the region where $j > 0$, $i+j \leq l'$ and $l'-l < i \leq \min\{l', n-l\}$.

Combining the six cases above, the probability of mutations from group l' to group l, $P[w_{l'\to l}]$, is given by

$$P[w_{l'\to l}] = P[\text{C1}]+P[\text{C2}]+P[\text{C3}]+P[\text{C4}]+P[\text{C5}]+P[\text{C6}]$$

Note that the expressions for all cases except $P[\text{C1}]$ have $i\ (S_*-1)$ terms in the denominator. For even moderate alphabet sizes these probabilities thus become very small compared to $P[\text{C1}]$ and can be neglected to a good degree of approximation. Thus $P[w_{l'\to l}] \approx P[\text{C1}] = P_m(n,l,l')$.

The time evolution of the l^{th} strain group is thus governed by the the rate of up-mutations from strain groups with lower Hamming distances. In each time unit, the strength of the strain group l' increases by $\beta A(l')w_{l'}(t)$ and a fraction $P[w_{l'\to l}]$ of these mutate to strain group l. Summing up these contributions, the time evolution of $w_l(t)$ is then given by

$$\frac{dw_l(t)}{dt} = \sum_{l'=0}^{l} P_m(n,l,l')\beta A(l')w_{l'}(t)$$

which completes the proof of Claim 1. □

REFERENCES

[1] J. Crandall et. al., "On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits," *Proc. ACM CCS,* 2005, pp. 235-248.

[2] C. Kruegel et. al., "Polymorphic Worm Detection Using Structural Information of Executables," *Proc. RAID,* 2005, pp. 207-226.

[3] Z. Li et. al., "Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience," *Proc. IEEE Symp. on S&P,* 2006, pp. 32-47.

[4] J. Newsome, B. Karp and D. Song, "Polygraph: Automatically Generating Signatures for Polymorphic Worms," *Proc. IEEE Symp. on S&P*, 2005, pp. 226-241.

[5] Y. Tang and S. Chen. "Defending Against Internet Worms: A Signature-Based Approach," *Proc. of IEEE INFOCOM*, 2005, pp. 1384-1393.

[6] J. Wang, I. Hamadeh, G. Kesidis and D. Miller, "Polymorphic worm detection and defense: system design, experimental methodology, and data resources," *Proc. ACM LSAD Workshop,* 2006, pp. 169-176.

[7] A. Pasupulati et. al. "Buttercup: on network-based detection of polymorphic buffer overflow vulnerabilities," *Proc. IEEE/IFIP NOMS,* 2004, pp. 235-248.

[8] M. Polychronakis, K. Anagnostakis and E. Markatos, "Network-level polymorphic shellcode detection using emulation," *Journal in Computer Virology,* vol. 2, no. 4, pp. 257-274, February 2007.

[9] P. Fogla et. al., "Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic," *Proc. USENIX Sec. Symp.,* 2006, pp. 17.

[10] R. Perdisci et. al., "Misleading Worm Signature Generators Using Deliberate Noise Injection," *Proc. IEEE SSP,* 2006, pp. 17-31.

[11] J. Newsome, B. Karp and D. Song, "Paragraph: Thwarting signature learning by training maliciously," *Proc. RAID,* 2006, pp. 81-105.

[12] Z. Chen, L. Gao and K. Kwait, "Modeling the spread of active worms," *Proceedings of IEEE INFOCOM,* 2003, pp. 1890-1900.

[13] C. Zou, D. Towsley and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm," *IEEE Trans. on Dependable and Secure Computing,* vol. 4, no. 2, pp. 105-118, April 2007.

[14] D. Moore, C. Shannon and K. Claffy, "Code-Red: A case study on the spread and victims of an Internet worm," *Proc. IMW,* 2002, pp. 273-284.

[15] D. Moore et. al., "Internet quarantine: Requirements for containing self-propagating code," *Proc. IEEE INFOCOM,* 2003, pp. 1901-1910.

[16] G. Vigna et. al., "Testing network based intrusion detection signatures using mutant exploits," *Proc. ACM CCS,* 2004, pp. 21-30.

[17] J. Tucek et. al., "Sweeper: A Lightweight End-to-End System for Defending Against Fast Worms," *Proc. of EuroSys Conference,* 2007, pp. 115-128.

[18] J. Jung, R. Milito and V. Paxson, "On the Adaptive Real-Time Detection of Fast-Propagating Network Worms," *Proc. DIMVA,* 2007, pp. 175-192.

[19] N. Weaver, S. Staniford and V. Paxson, "Very Fast Containment of Scanning Worms," *Proc. USENIX Sec. Symp.,* pp. 29-44, 2004.

[20] H. Kim and B. Karp, "Autograph: toward automated, distributed worm signature detection," *Proc. USENIX Sec. Symp.,* 2004, pp. 271-286.

[21] H. Yin et. al., "Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis," *Proc. ACM CCS,* 2007, pp. 116-127.

[22] K. Wang, G. Cretu and S. Stolfo, "Anomalous Payload-Based Worm Detection and Signature Generation," *Proc. RAID,* 2006, pp. 227-246.

[23] M. Nilsson and N. Snoad, "Error thresholds for quasispecies on dynamic fitness landscapes," *Physical Review Letters,* vol. 84, no. 1, pp. 191-194, January 2000.

[24] C. Kamp and S. Bornholdt, "Coevolution of quasispecies: B-cell mutation rates maximize viral error catastrophes," *Physical Review Letters,* vol. 88, no. 6, pp. 068104.1-068104.4, February 2002.

[25] C. Nachenberg, "Computer virus-antivirus coevolution," *Communications of the ACM,* vol. 40. no. 1, pp. 46-51, January 1997.

[26] D. Brumley et. al., "Towards automatic generation of vulnerability-based signatures," *Proc. IEEE Symp. on S&P,* 2006, pp. 2-16.

[27] M. Chouchane, A. Walenstein and A. Lakhotia, "Statistical Signatures for Fast Filtering of Instruction-substituting Metamorphic Malware," *Proc. ACM WORM,* 2007.

[28] S. Chung and A. Mok, "Allergy attack against automatic signature generation," *Proc. of RAID,* Hamburg, Germany, September, 2006, pp. 61-80.

[29] B. Stephenson and B. Sikdar, "A quasi-species approach for modeling the dynamics of polymorphic worms," *Proc. IEEE INFOCOM,* 2006, pp. 1-12.

[30] S. Staniford, V. Paxson and N. Weaver, "How to own the Internet in your spare time," *Proc. USENIX Sec. Symp.,* 2002, pp. 149-167.

[31] K2, ADMmutate. `http://www.ktwo.ca/c/ADMmutate-0.8.4.tar.gz`.