

Using Signal Processing Techniques to Model Worm Propagation over Wireless Sensor Networks

Computer worms have recently emerged as one of the most imminent and effective threats against information confidentiality, integrity, and service availability. Internet worms have repeatedly revealed the susceptibility of Internet hosts to malicious intrusions by compromising millions of vulnerable hosts at an extremely fast pace [1]–[3]. Some recent studies (see, for example, [3]) have shown that antiworms (also referred to as good worms) can serve as an effective counterattack tool by spreading disinfection and immunization information in the same manner as malicious worms. The antiworms can, hence, be employed to disseminate security-critical information at a very fast pace.

An accurate propagation model is instrumental to understand the automated spread of a worm [1]–[3]. Worm propagation models also facilitate the design of real-time detection strategies. The battery-constrained, time-critical, and military-oriented natures of many sensor networks necessitate a robust security framework. Design of secure sensor networks should therefore consider real-time monitoring, detection and mitigation of malicious worms. An accurate model is necessary to characterize and evaluate propagation of worms over sensor networks. In this article, we derive a novel and accurate worm propagation model for wireless sensor networks. Referred to as a topologically aware worm propagation model (TWPM), this model simultaneously captures the time and space dynamics of worms spreading over a sensor network. (Note that the term *topologically aware scanning* was introduced by Staniford et al. in their seminal study to refer to

worms “which use information available on a victim’s machine to select new targets” [1].)

In this article, we define worm propagation characteristics that are specific to sensor networks. We parameterize the effects of physical channel conditions, medium access control (MAC) layer contention, network layer routing, and transport layer protocol on worm propagation in sensor networks. These parameters are incorporated in the TWPM, which borrows its basic formulation from models of epidemic diseases [4]. The advanced model parameters and the mathematical treatment following the formulation are then developed specifically for sensor networks. The basic model formulation results in a partial differential equation, which is solved in the frequency domain to yield a closed-form solution for the TWPM. It is shown that in the spatial domain the TWPM spread function is low-pass filtered by a two-dimensional (2-D) isotropic Gaussian filter, thereby providing an intuitive feel for the dependence of the model on its underlying (physical, MAC, and network layer) parameters. For performance evaluation, we simulate the spread of a worm over a sensor network. The simulated and TWPM-predicted worm propagation dynamics are then compared to evaluate the accuracy of the model. We show that the TWPM predicts the worm propagation dynamics very accurately.

SENSOR NETWORK PROPAGATION PARAMETERS AND ASSUMPTIONS

In this section, we state the assumptions made in this work and define new worm propagation parameters which arise due to the inherent attributes of a sensor network.

SYSTEM DESCRIPTION

We consider a network composed of N stationary and identical sensors which are placed on a rectangular 2-D grid. The sensors are equipped with omnidirectional antennas that have a maximum transmission range of r meters. The horizontal and vertical axes are represented by ξ and η , respectively. To simplify analysis, we uniformly (and logically) sample both axes and treat ξ and η as discrete variables. Each discrete (ξ, η) position is referred to as a segment. Let l and h denote the length and height of a segment, respectively. Here, it should be emphasized that this segmentation is only logical with just one constraint: $r \ll l \times h$. Due to this constraint, a sensor in segment (ξ, η) can receive traffic from sensors in the same segment (ξ, η) or (at maximum) from sensors in neighboring segments of (ξ, η) . The neighboring segments of segment (ξ, η) are shown in Figure 1.

The distribution of sensors on the grid is governed by a 2-D, discrete-time random process $\mathfrak{S}(\xi, \eta)$. Each constituent random variable of $\mathfrak{S}(\xi, \eta)$ describes the number of sensors in the (ξ, η) segment. The random variables of $\mathfrak{S}(\xi, \eta)$ are assumed to be independent and identically distributed (IID). Using the IID assumption, let $E\{\mathfrak{S}(\xi, \eta)\} = \mu_D$ represent the expected value of $\mathfrak{S}(\xi, \eta)$ for any ξ, η . Then, on-average, we have

$$\begin{aligned} &\text{average number of nodes} \\ &\text{per segment} = \mu_D. \end{aligned} \quad (1)$$

We assume that the sensors in a segment are distributed (located) uniformly within the boundaries of the segment. Figure 1 outlines the fact that, due to the $r \ll l \times h$ constraint,

sensors on the edges of a segment can communicate with sensor in parts of the neighboring segments. In essence, a sensor in segment (ξ, η) can only communicate with sensors inside the thick, broken line of Figure 1. For instance, the sensor located at the corner of the (ξ, η) segment can at most send/receive traffic to/from sensors within its transmission range, as represented by the circle in Figure 1.

PHYSICAL LAYER PARAMETERS

To simultaneously capture distance- and fading-based attenuations in the wireless medium, we employ a log-normal shadow fading model [5] to define the probability that a transmitted packet is successfully received in a sensor network. Previous studies (see for example [6]) have illustrated the efficacy of this channel model in defining ad hoc network topologies. We assume that channel conditions do not change drastically during transmission of a given infectious packet. The conditions can, however, change for different packets.

Consider two nodes u and v at a distance $d(u, v)$ from each other. The signal attenuation between the two nodes is then expressed as $\beta(u, v) = 10 \log(p_t/p_r)$ dB, where p_t and p_r , respectively, represent the transmitted and received powers and $p_r \leq p_t$. In a shadow fading environment, $\beta(u, v)$ comprises two additive components: $\beta(u, v) = \beta_1(u, v) + \beta_2$. The first component is a deterministic distance dependent variable defined as

$$\beta_1(u, v) = \alpha 10 \log(d(u, v)) \text{ dB}, \quad (2)$$

where α is a path loss exponent that depends on the environment (generally $2 \leq \alpha \leq 5$). The second component, β_2 , captures the fading effects and is defined as a normal random variable with zero mean and variance σ^2

$$f_{\beta_2}(\beta_2) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{\beta_2^2}{2\sigma^2}\right). \quad (3)$$

A packet transmission between nodes u and v is successful if the

received signal power, p_r , is greater than or equal to a certain threshold power $p_{r,th}$. In other words, given a receiver sensitivity $p_r \geq p_{r,th}$, a packet transmission from u to v is successful if the signal attenuation between u and v is constrained by $\beta(u, v) \leq \beta_{th}$, where the threshold attenuation is $\beta_{th} = 10 \log(p_t/p_{r,th})$ dB. The probability of successful transmission between nodes u and v in the presence of shadow fading can then be expressed as

$$p = \Pr\{\beta(u, v) \leq \beta_{th}\} \\ = \int_{-\infty}^{\beta_{th}-\beta_a} \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{\beta_2^2}{2\sigma^2}\right) d\beta_2.$$

Let $\beta_2/\sqrt{2}\sigma = x$ which gives $d\beta_2 = \sqrt{2}\sigma dx$ and the upper integral limit becomes $x = (\beta_{th} - \beta_a)/\sqrt{2}\sigma$. Using x as the variable of integration yields

$$p = \int_{-\infty}^{\frac{\beta_{th}-\beta_a}{\sqrt{2}\sigma}} \frac{1}{\sqrt{\pi}} \exp(-x^2) dx.$$

Employing the symmetry of the normal distribution we get

$$p = \frac{1}{2} + \int_0^{\frac{\beta_{th}-\beta_a}{\sqrt{2}\sigma}} \frac{1}{\sqrt{\pi}} \exp(-x^2) dx.$$

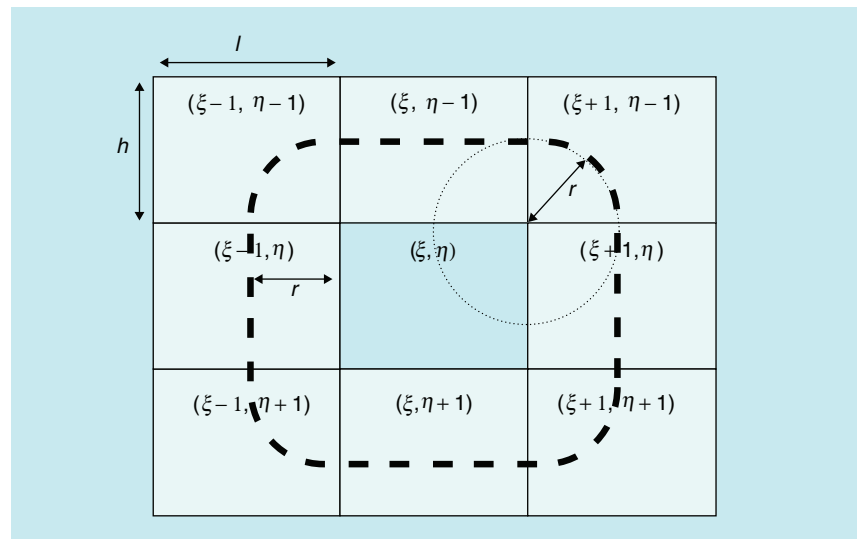
Expressing the probability using the error function and plugging in the value of $\beta_1(u, v)$ from (2), the probability of a

successful packet transmission between u and v can be written as

$$p = \frac{1}{2} + \frac{1}{2} \operatorname{erf} \left(\frac{\beta_{th} - \alpha 10 \log(d(u, v))}{\sqrt{2}\sigma} \right). \quad (4)$$

MAC LAYER PARAMETERS

As opposed to the Internet, worms over sensor networks will face channel contention, which should in theory reduce the overall rate of spread. Depending on the node density and MAC layer fairness, the highest achievable probe rate might be significantly lower than the Internet. A similar trend has been observed for Internet worms, where after the initial fast spread phase, worm traffic causes severe congestion at routers and, hence, the spread rate decreases. In view of the added constraint of MAC contention, sensor network worms (good or malicious) should be more bandwidth- and contention-aware than Internet worms. We assume that, to avoid unsuccessful transmissions, the sensors employ a carrier sense multiple access with collision avoidance (CSMA/CA) mechanism with handshaking. Thus, while we account for channel contention, it is assumed that packet transmissions are collision



[FIG1] Neighbors of segment (ξ, η) .

free. Let there be $N(\xi, \eta)$ nodes in segment (ξ, η) . Then $N'(\xi, \eta) \leq N(\xi, \eta)$ nodes can be granted simultaneous channel access in the segment.

NETWORK AND TRANSPORT LAYER CONSIDERATIONS

An effective virulence strategy, referred to as localized scanning, has been employed by recent Internet worms. After compromising a host, local scanning worms scan the nearby hosts (e.g., machines in the same subnet) with a higher probability. In the localized scanning context, a sensor network worm has an invaluable resource available to it in the form of its next-hop neighbor list. We assume that neighbor list is maintained at each node. An infectious sensor can spread the infection quite effectively by communicating it only to its next-hop neighbors. This strategy, which we refer to as next-hop scanning, will provide effective worm propagation with minimal channel contention delays. It should be emphasized here that despite the negative meaning associated with the term infectious (and, consequently, the term infected), in this article infectious/infected sensor refers to a node that has received the worm payload and is actively participating in spreading the payload. No assumption is made about the intent of the infectious payload. Throughout this article we assume that the worm employs the next-hop infection strategy. Since the worm under consideration employs (next-hop) information from a host to infect other hosts, we refer to it as a topologically aware worm [1].

Recent highly virulent worms are employing datagram communications due to the low protocol overhead and the consequent lower bandwidth consumption. (Note that the Witty worm [2], which has the fastest spread rate among all worms to date, had a user datagram protocol (UDP) payload.) In this article, we also assume that infections are transmitted using the UDP. A node can receive multiple infectious packets from different transmitters. An infected node communicates the infection to its neighbors only once.

WORM PROPERTIES

We focus on unknown worms, which have also been referred to as zero-day worms and novel worms in previous literature. For the malicious worm case, we assume that high virulence and unknown nature of the present next-hop worm renders immunization ineffective. We also assume a constant infection rate for the next-hop scanning sensor network worm.

THE TOPOLOGICALLY AWARE WORM PROPAGATION MODEL

Using the parameters defined in the last section, we now describe the TWPM.

TWPM FORMULATION

We focus solely on propagation dynamics of unknown worms. Therefore, a node can be in one of two possible states: susceptible or infected. We emphasize again that the term infected simply refers to a node which has received the worm payload, without any assumption about the (good or bad) intent of the payload. A susceptible node becomes infected as soon as it is contacted by an infectious node. Immediately after becoming infected, a node begins spreading the worm. Let the total number of susceptible and infectious nodes in segment (ξ, η) at time t be denoted by $S(\xi, \eta, t)$ and $I(\xi, \eta, t)$, respectively. Using average statistics, the sum of nodes in both states should be

$$S(\xi, \eta, t) + I(\xi, \eta, t) = \mu_D, \quad (5)$$

where μ_D represents the average number of sensors in a segment as defined in (1). This model is referred to as the classical susceptible infected (SI) model of epidemic diseases [4]. The rate of change of susceptible population with respect to time can then be expressed as [4]

$$\frac{\partial S(\xi, \eta, t)}{\partial t} = -\beta S(\xi, \eta, t) I(\xi, \eta, t), \quad (6)$$

where $0 < \beta \leq 1$ represents the constant infection rate. We assume that the total population of initially susceptible nodes is large enough so that during the initial stages of the worm spread, the susceptible population is approximately constant. More specifically, an infectious node can infect $\beta S(\xi, \eta, t)$ susceptible nodes in one unit of time. Thus, $I(\xi, \eta, t)$ infectious nodes can create a total of $\beta S(\xi, \eta, t) I(\xi, \eta, t)$ new infections in each time unit. However, in accordance with our earlier discussion, channel conditions and contention will reduce the virulence of the worm. Specifically, $I(\xi, \eta, t)$ infectious nodes will create a total of $p\beta N'(\xi, \eta) I(\xi, \eta, t)$ new infections in each time unit, where p is the probability of successful packet transmission and $N'(\xi, \eta)$ is the number of nodes in segment (ξ, η) that can receive a packet (despite channel contention) in one time unit; note that $N'(\xi, \eta) \leq N(\xi, \eta)$ so on average $N'(\xi, \eta) \leq \mu_D$. Let us denote the rate of infectious contacts received from neighboring segments of (ξ, η) as ϕ , where $\phi \leq \beta$ since all of the infectious contacts from a neighboring segment are not targeted at segment (ξ, η) .

A closer look at Figure 1 shows that if a sensor is located exactly at one of the corners of the (ξ, η) segment, then at maximum it can receive an infectious contact from a node that is at distance r from it (shown by the circle). For instance, at most, infected nodes from segment $(\xi - 1, \eta - 1)$ that are within $\pi r^2/4$ area of the corner of (ξ, η) can spread infection to nodes in segment (ξ, η) . Since the total area of a segment is $l \times h$, and since nodes are uniformly distributed inside a segment, a total of $\phi p(\pi r^2/4lh)N'(\xi - 1, \eta - 1) \times I(\xi - 1, \eta - 1)$ infectious contacts are received by segment (ξ, η) from the neighboring segment $(\xi - 1, \eta - 1)$. By similar logic, infected nodes of segment $(\xi, \eta - 1)$ will transmit $\phi p(r/lh)N'(\xi, \eta - 1)I(\xi, \eta - 1)$ to the (ξ, η) segment. Infections from the remaining segments can be expressed in a similar manner. Thus the rate of change in the infectious population is

$$\begin{aligned}
\frac{\partial I(\xi, \eta, t)}{\partial t} = & \beta p N'(\xi, \eta) I(\xi, \eta, t) \\
& + \phi p \frac{r}{h} N'(\xi, \eta) \\
& \times [I(\xi - 1, \eta, t) \\
& + I(\xi + 1, \eta, t) \\
& + I(\xi, \eta + 1, t) \\
& + I(\xi, \eta - 1, t)] \\
& + \phi p \frac{\pi r^2}{4lh} N'(\xi, \eta) \\
& \times [I(\xi - 1, \eta - 1, t) \\
& + I(\xi + 1, \eta - 1, t) \\
& + I(\xi - 1, \eta + 1, t) \\
& + I(\xi + 1, \eta + 1, t)]. \tag{7}
\end{aligned}$$

Now that we have defined the basic equations, we focus on obtaining a closed-form solution for the above model. Previous studies of Internet worm epidemics have outlined that the spread is exponential during the initial stages [1], [2]. We are, therefore, particularly interested in ascertaining the solution for $I(\xi, \eta, t)$ during initial stages of the worm outbreak. The next section derives the closed-form solution.

SIMPLIFICATION IN FREQUENCY DOMAIN

The expression for TWPM given in (7) is somewhat convoluted. To simplify this expression, let us rewrite (7) as

$$\begin{aligned}
\frac{\partial I(\xi, \eta, t)}{\partial t} = & AI(\xi, \eta, t) \\
& + \frac{B}{2} [I(\xi - 1, \eta - 1, t) \\
& + I(\xi + 1, \eta - 1, t) \\
& + I(\xi - 1, \eta + 1, t) \\
& + I(\xi + 1, \eta + 1, t)] \\
& + \frac{C}{2} [I(\xi - 1, \eta, t) \\
& + I(\xi + 1, \eta, t) \\
& + I(\xi, \eta + 1, t) \\
& + I(\xi, \eta - 1, t)],
\end{aligned}$$

where

$$\begin{aligned}
A &= \beta p N'(\xi, \eta) \\
B &= \phi p (\pi r^2 / 2lh) N'(\xi, \eta) \text{ and} \\
C &= 2\phi p (r/h) N'(\xi, \eta).
\end{aligned}$$

To solve this partial differential equation, we take a 2-D discrete-time Fourier transform (DTFT) along the ξ and η axes. Two points should be highlighted here. i) DTFT is taken on the spatial variables, ξ and η , rather than the conventional time, t , variable. Hence, the transform is in fact a discrete-space Fourier transform. We employ the term DTFT since it is a commonly used term that the readers can relate to. It should be kept in mind, however, that the transform is being taken on the spatial variables. ii) To simplify the frequency domain analysis, we assume that $N'(\xi, \eta)$ does not change significantly from one segment to another. Hence, the parameter $N'(\xi, \eta)$ is not a function of the space variables $N'(\xi, \eta) = N'$, and consequently the parameters A , B , and C will be treated as constants when performing DTFT and inverse DTFT. Using $M(\omega, \theta, t)$ to denote the DTFT of $I(\xi, \eta, t)$, we obtain

$$\begin{aligned}
\frac{\partial M(\omega, \theta, t)}{\partial t} = & AM(\omega, \theta, t) \\
& + \frac{B}{2} M(\omega, \theta, t) \\
& \times (e^{-j(\omega+\theta)} + e^{j(\omega-\theta)} \\
& + e^{-j(\omega-\theta)} + e^{j(\omega+\theta)}) \\
& + \frac{C}{2} M(\omega, \theta, t) \\
& \times (e^{-j\omega} + e^{j\omega} \\
& + e^{j\theta} + e^{-j\theta}),
\end{aligned}$$

which can be expressed as

$$\begin{aligned}
\frac{\partial M(\omega, \theta, t)}{\partial t} = & [A + B(\cos(\omega + \theta) \\
& + \cos(\omega - \theta)) \\
& + C(\cos(\omega) + \cos(\theta))] \\
& \times M(\omega, \theta, t).
\end{aligned}$$

Assuming that the infection starts with a single infectious node (the initial condition), the solution for the above differential equation is

$$\begin{aligned}
M(\omega, \theta, t) = & \exp \{At + Ct(\cos(\omega) \\
& + \cos(\theta)) \\
& + Bt(\cos(\omega + \theta) \\
& + \cos(\omega - \theta))\}. \tag{8}
\end{aligned}$$

The exponent in the above expression is mathematically cumbersome and, hence, we employ the Taylor series approximation of the cosine function given by $\cos(\omega) = 1 - (\omega^2/2!) + (\omega^4/4!) - (\omega^6/6!) + \dots$. Using the first two terms of the above expansion, an approximation of $M(\omega, \theta, t)$ can be written as

$$\begin{aligned}
M(\omega, \theta, t) \approx & \exp \left\{ At + Ct \right. \\
& \times \left(1 - \frac{\omega^2}{2} + 1 - \frac{\theta^2}{2} \right) \\
& + Bt \left(1 - \frac{(\omega - \theta)^2}{2} \right. \\
& \left. \left. + 1 - \frac{(\omega + \theta)^2}{2} \right) \right\} \\
\approx & \exp \left\{ t(A + 2B + 2C) \right. \\
& - \omega^2 t \left(B + \frac{C}{2} \right) \\
& \left. - \theta^2 t \left(B + \frac{C}{2} \right) \right\}.
\end{aligned}$$

Let $1/(2F) = t(B + (C/2))$ and the above expression becomes

$$\begin{aligned}
M(\omega, \theta, t) \approx & \exp \{t(A + 2B + 2C)\} \\
& \exp \left\{ -\frac{\omega^2 + \theta^2}{2F} \right\}. \tag{9}
\end{aligned}$$

A close look at the above expression reveals that the first exponent in (9) is being multiplied by a 2-D isotropic (i.e., circularly symmetric) Gaussian function. Since the Fourier transform of a Gaussian is also a Gaussian, this multiplication in the frequency domain corresponds to a convolution with a Gaussian function in the spatial domain. Thus, the number of infected nodes in a segment at a given time is filtered by a (low-pass) isotropic Gaussian spatial filter. From (9), the standard deviation of the Gaussian filter in the frequency domain is

$$\begin{aligned}\sigma_{\text{freq}} &= \sqrt{F} \\ &= \frac{1}{\sqrt{tp\phi N' \left(\frac{\pi r^2}{lh} + 2\frac{r}{h} \right)}}.\end{aligned}\quad (10)$$

From (10), it is clear that at a given time the standard deviation of the filter in the frequency domain is inversely proportional to the probability of successful transmission p , the number of nodes in the segment that can access the medium in the given time slot N' , and the transmission ranges of the nodes r . The variance of a time domain Gaussian function is inversely proportional to its frequency domain counterpart [7]. Hence, the standard deviation (or bandwidth) of this Gaussian filter in the spatial domain, σ_{space} , is in fact directly proportional to p , N' and r . In other words, the number of infected nodes in a segment is directly proportional to p , N' , and r . This result, although unsurprising, gives an intuitive feel for the interdependence of the number of infected nodes in a segment and the underlying TWPM parameters.

FINAL CLOSED-FORM SOLUTION

We now revert to the original frequency domain expression of the TWPM given in (9) and provide the final closed-form solution in the spatial domain. Taking the inverse DTFT of (9) gives

$$\begin{aligned}I(\xi, \eta, t) &\approx e^{t(A+2B+2C)} \\ &\int \int e^{-\frac{\omega^2 + \theta^2}{2F}} e^{j\xi\omega + j\eta\theta} d\omega d\theta \\ &\approx e^{t(A+2B+2C)} \int e^{-\frac{\omega^2}{2F}} e^{j\xi\omega} d\omega \\ &\int e^{-\frac{\theta^2}{2F}} e^{j\eta\theta} d\theta.\end{aligned}$$

The forward Fourier transform of the Gaussian function $e^{-(\xi^2/2F)}$ is given by $\sqrt{2\pi F} e^{-F\omega^2/2}$. By duality we obtain

$$\sqrt{2\pi F} e^{-F\xi^2/2} \xleftrightarrow{DTFT} 2\pi e^{-\frac{\omega^2}{2F}}$$

or

$$\sqrt{\frac{F}{2\pi}} e^{-F\xi^2/2} \xleftrightarrow{DTFT} e^{-\frac{\omega^2}{2F}}.$$

Using this expression for inverse DTFT we get

$$I(\xi, \eta, t) \approx \frac{F}{2\pi} e^{t(A+2B+2C)} e^{-F\xi^2/2} e^{-F\eta^2/2}.$$

Plugging in the values of A , B , C , and F renders the final approximate closed-form expression as

$$\begin{aligned}I(\xi, \eta, t) &\approx \frac{1}{2\pi t\phi p N' \left(\frac{\pi r^2}{lh} + \frac{2r}{h} \right)} \\ &\times \exp \left\{ tp N' \left(\beta + \phi \frac{\pi r^2}{lh} \right. \right. \\ &\quad \left. \left. + 4\phi \frac{r}{h} \right) \right\} \\ &\times \exp \left\{ \frac{-\xi^2 - \eta^2}{2tp\phi N' \left(\frac{\pi r^2}{lh} + \frac{2r}{h} \right)} \right\}.\end{aligned}\quad (11)$$

The above expression gives a closed-form solution for the TWPM. The first exponential term shows that the initial spread is an exponential function of the infection rate, β , and the channel contention, represented by N' , in the current segment. The $e^{\phi t}$ terms in the first exponent emphasize that the number of infectious contacts ϕ received from neighboring segments further expedite the infection process in the current segment. The second exponent in (11) exponentially decreases with an increase in ξ or η . This result is intuitive since nodes that are spatially far away from the infectious concentration are much less likely to contract infections. Thus, the number of infectious nodes in a segment ξ, η is a function of its distance from the infectious concentration.

SIMULATION RESULTS

We developed a simulator that can abstractly simulate worm traffic over a sensor network. Given the total number of nodes, a 2-D grid size and a random distribution, the simulator placed the nodes on the grid using the random distribution as the constituent distribution of a 2-D IID process. Once

the transmission range of each node was specified, the simulator calculated the next-hop neighbors using the Euclidean distance measure. The following parameters comprise the input of the simulator: 1) infection rate β , 2) maximum nodes in a segment that can access the channel in a given time unit, N' , and 3) threshold attenuation and path-loss exponent.

At each time instance, every infected node communicated the infection to β fraction of its neighbors. The receiver node simulated the fading effects by generating a Gaussian random variable. A transmitted packet was dropped or received at the receiver on the basis of the level of (simulated) channel attenuation. Some of the nodes received multiple infections through different neighbors. The simulator generated worm propagation traces for the total number of infected sensors in the grid.

We performed many experiments with varying parameters. It was observed that the model followed the simulation results quite closely. As an example, in Figure 2 we show results from a simulation on a 250×250 m² grid with $N = 25,000$ sensors. Other parameters include: $r = 3$ m, $p = 0.95$, $\alpha = 2$, $l = h = 10$ m, and $N' = \mu_D = 40$.

The total number of infected nodes at different time instances is shown for two infection rates, $\beta = \phi = 0.2$ and $\beta = \phi = 0.5$, in Figure 2. The results in Figure 2 are plotted against normalized times of the TWPM-predicted and simulated worm propagations. It can be seen that the TWPM follows the simulation results quite accurately, especially during the initial and final stages of the infection. Even during the intermediate stages, the TWPM performance is quite close to the simulation results. Thus, we conclude that the TWPM provides an accurate model for worm propagation in a sensor network.

Figure 2 also reveals that the TWPM is quite similar to the spread of Internet worms, i.e., an exponential initial spread followed by a linear increase and, finally, a slow spread. This similarity between the worm spread dynamics

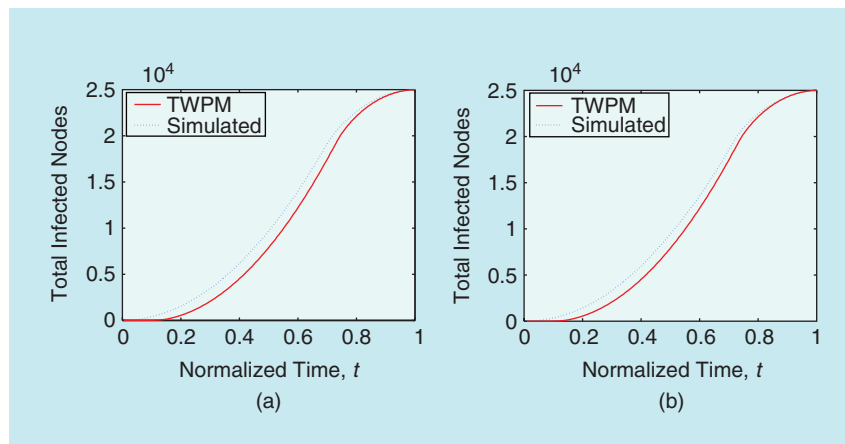
over a sensor network and the Internet can be explained as follows. The exponential initial spread of Internet worms is due to the availability of large numbers of vulnerable hosts. Since we are modeling an unknown (zero-day) worm, even in the sensor network case, the initial size of the susceptible population is quite large, which results in a fast initial increase. Similar to the Internet, as time progresses, more and more susceptible sensors are infected and therefore the curve assumes a linear increase. The slow final spread in the Internet was attributed to the fact that few vulnerable hosts remain, and it takes more time to search out these vulnerable hosts. The explanation for the slow final spread of sensor networks has precisely the same explanation; that is, in the last stages of the infection almost all sensors are surrounded by neighbors that are already infected, thereby resulting in a slow spread.

CONCLUSION

In this article, we formulated and derived a topologically aware worm propagation model for wireless sensor networks. Simulation results demonstrated that the TWPM provides an effective and accurate worm propagation model for sensor networks.

ACKNOWLEDGMENTS

The authors thank the anonymous reviewer of this article for providing his/her valuable feedback. The authors thank the National Science Foundation (NSF) for supporting this project. This material is based upon work supported by the NSF under NSF CyberTrust Grant No. 0430436. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF. Finally, the authors would like to thank Wajahat Ali Syed for his helpful comments on the original manuscript of this article.



[FIG2] Total number of infections given by TWPM and simulation: (a) $\beta = 0.2$, (b) $\beta = 0.5$.

AUTHORS

Syed A. Khayam received the B.S. degree in computer systems engineering from National University of Sciences and Technology (NUST), Pakistan, in 1999 and his M.S. degree in electrical engineering from Michigan State University in 2003, where he is currently a Ph.D. candidate. He also worked at Communications Enabling Technologies. His research interests include statistical analysis and modeling of computer networks, network security, cross-layer protocol design, real-time multimedia communications over IP-based networks, and VLSI chip design.

Hayder Radha received the B.S. degree (with honors) from Michigan State University (MSU) in 1984, the M.S. degree from Purdue University in 1986, and the Ph.M. and Ph.D. degrees from Columbia University in 1991 and 1993, respectively (all in electrical engineering). He joined MSU in 2000 as associate professor in the Department of Electrical and Computer Engineering. From 1986–1996, he was with Bell Laboratories. From 1996–2000, he worked at Philips Research USA and became a Philips Research Fellow in 2000. His research interests include wireless and multimedia communications and networking, stochastic model-

ing, and image and video coding and compression. He has more than 25 patents in these areas. He served as cochair and editor of the ATM and LAN Video Coding Experts Group of the ITU-T in 1994–1996. He is a member of the IEEE Signal Processing Multimedia Technical Committee. He is a recipient of the Bell Labs Distinguished Member of Technical Staff Award (1993), the Withrow Distinguished Scholar Award (2003), and the Microsoft Research Content and Curriculum Award (2004).

REFERENCES

- [1] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in your spare time," in *Proc. Usenix Security Symp.*, 2002, pp. 149–167.
- [2] C. Shannon and D. Moore, "The spread of the Witty worm," *IEEE Security & Privacy*, vol. 2, no. 4, July/Aug. 2004, p. 46–50.
- [3] F. Castaeda, E.C. Sezer, and J. Xu, "WORM vs. WORM: A preliminary study of an active counter-attack mechanism," in *Proc. ACM Int. Workshop Rapid Malcode (WORM)*, Oct. 2004, p. 83–93.
- [4] N.T.J. Bailey, *The Mathematical Theory of Infectious Diseases and Its Applications*. London: Charles Griffin & Co., 1975.
- [5] T.S. Rappaport, *Wireless Communications: Principles and Practice*, 2 ed. Englewood Cliffs, NJ: Prentice-Hall, 2001.
- [6] C. Bettstetter and C. Hartmann, "Connectivity of wireless multihop networks in a shadow fading environment," in *Proc. ACM Int. Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*, Sep. 2003, p. 28–32.
- [7] B.P. Lathi, *Signal Processing and Linear Systems*. New York: Oxford Univ. Press, 1998. **SP**