OPEN ACCESS

Worm epidemics in wireless ad hoc networks

New Journal of Physics
The open–access journal for physics

Worm epidemics in wireless ad hoc networks

Maziar Nekovee
BT Research, Polaris 134, Adastral Park, Martlesham, Suffolk IP5 3RE, UK
and
Centre for Computational Science, University College London,
20 Gordon Street, London WC1H 0AJ, UK
E-mail: maziar.nekovee@bt.com

New Journal of Physics **9** (2007) 189
Received 13 March 2007
Published 28 June 2007
Online at http://www.njp.org/
doi:10.1088/1367-2630/9/6/189

Abstract. A dramatic increase in the number of computing devices with wireless communication capability has resulted in the emergence of a new class of computer worms which specifically target such devices. The most striking feature of these worms is that they do not require Internet connectivity for their propagation but can spread directly from device to device using a short-range radio communication technology, such as WiFi or Bluetooth. In this paper, we develop a new model for epidemic spreading of these worms and investigate their spreading in wireless ad hoc networks via extensive Monte Carlo simulations. Our studies show that the threshold behaviour and dynamics of worm epidemics in these networks are greatly affected by a combination of spatial and temporal correlations which characterize these networks, and are significantly different from the previously studied epidemics in the Internet.

PII: S1367-2630(07)46115-8

Contents

1. Introduction

Worms are self-replicating computer viruses which can propagate through computer networks without any human intervention [1]–[3]. Cyber attacks by this type of viruses present one of the most dangerous threats to the security and integrity of computer and telecommunications networks. The Code Red [4, 5] and Nimda [4] worms, for example, infected hundreds of thousands of computers at alarming speeds and the resulting worm epidemics cost both the public and the private sector a great deal of money. The last few years have seen the emergence of a new type of worms which specifically targets portable computing devices, such as smartphones and laptops. The novel feature of these worms is that they do not necessarily require Internet connectivity for their propagation. They can spread directly from device to device using a short-range wireless communication technology, such as WiFi or Bluetooth [4, 6, 7], creating in their wake an ad hoc contact network along which they propagate. The first computer worm written specially for wireless devices was detected in 2003 and within three years the number of such viruses soared from one to more than 300 (For a recent review, see [8]). With wireless networks becoming increasingly popular, many security experts predict that these networks will soon be a main target of attacks by worms and other type of malware [8].

Worm and virus attacks on the Internet have been the subject of extensive empirical, theoretical and simulation studies [1], [9]–[12]. These studies have greatly contributed to our understanding of the impact of network topology on the properties of virus spreading [9, 10] and have inspired the design of more effective immunization strategies to prevent and combat Internet epidemics [11, 12]. Investigation of virus spreading in wireless networks in general and worms in particular is, however, in its infancy, and there have been very limited studies which address this problem [7, 13].

In this paper, we develop a new model for the spreading of worms in WiFi-based wireless ad hoc networks and investigate the properties of worm epidemics in these networks via extensive Monte Carlo simulations. Wireless ad hoc networks [14]–[18] are distributed networks which can be formed on the fly by WiFi-equipped devices, such as laptops and smartphones. Nodes in these networks communicate directly with each other and can route data packets wirelessly,

either among themselves or to the nearest Internet access point. Ad hoc technology has important applications in the provisioning of ubiquitous wireless Internet access, disaster relief operations and wireless sensor networks. From the perspective of complex network theory [19]–[22] the study of these networks is important as their topology provides a clear-cut example of spatial networks [23]. Spatial networks are embedded in a metric space where interactions between the nodes is a function of their spatial distance [23, 24]. Despite their relevance to many real-life phenomena the properties of these networks are much less studied than abstract graphs.

Our Monte Carlo simulations show that epidemic spreading in wireless ad hoc networks is significantly different from the previously studied epidemics in the Internet. The initial growth of the epidemic is significantly slower than the exponential growth observed for worm spreading in the Internet, and the epidemic prevalence exhibits a density-dependent critical threshold which is higher than the value predicted by the mean-field theory. We show that these differences are due to strong spatial and temporal correlations which characterise these networks. Our study also reveals the presence of a self-throttling effect in the spreading of worms in wireless networks which greatly slows down the speed of worm invasion in these networks.

The rest of this paper is organized as follows. In section 2, we describe our models of network topology, data communication mechanism, and worm spreading in wireless ad hoc networks. In section 3, we present and discuss results of our Monte Carlo simulations studies of epidemics in these networks for a range of device densities and infection rates. We close this paper in section 4 with conclusions.

2. Models

2.1. Network model

We consider a collection of nodes distributed in a two-dimensional plane which communicate using short-range radio transmissions. The received radio signal strength at a device j resulting from a transmission by a device i decays with the distance between the sender and the receiver due to a combination of free-space attenuation and fading effects. Phenomenologically this effect is described using the so-called pathloss model [25] which states that the mean value of the signal power at a receiving device j is related to the signal power of the transmitting node i via the following equation:

$$P^{ij} = \frac{P^i}{cr_{ij}^{\alpha}}. \tag{1}$$

In the above equation r_{ij} is the Euclidean distance between node i and node j, P^i and P^{ij} are the transmit power and the received power, respectively, and c is a constant whose precise value depends on a number of factors including the transmission frequency. For free space propagation $\alpha = 2$, but depending on the specific indoor/outdoor propagation scenario it is found empirically that α can vary typically between 2 and 5. A data transmission by node i is correctly received at node j, i.e. i can establish a communication link with j, provided that:

$$\frac{P^{ij}}{\nu} = \frac{P^i/cr_{ij}^{\alpha}}{\nu} \geqslant \beta_{\text{th}}. \tag{2}$$

In the above equation β_{th} is an attenuation threshold and ν is the noise level at node j.

Condition (2) translates into a maximum transmission range for node i:

$$r_t^i = \left(\frac{P^i}{c\beta_{\text{th}}\nu}\right)^{1/\alpha}, \tag{3}$$

such that each device can establish wireless links with only those devices within a circle of radius r_t^i. A communication graph is then constructed by creating an edge between node i and all other nodes in the plane that are within the transmission range of i, and repeating this procedure for all nodes in the network. In general wireless devices may use different transmit powers such that the existence of a wireless link from i to j does not imply that a link from j to i also exists. Consequently the resulting communication graph is *directed*. Assuming, however, that all devices use the same transmit power P, and a corresponding transmission range r_t, the topology of the resulting network can be described as a two-dimensional random geometric graph (RGG) [26, 27]. RGGs have been used extensively in the study of continuum percolation and more recently for modelling wireless ad hoc networks [15]–[18], [28]. Like Erdős–Rényi random graphs (RG) [29], these graphs have a binomial degree distribution, $P(k)$, which peaks at an average value $\langle k\rangle$ and shows small fluctuations around $\langle k\rangle$. However, other properties of a RGG are radically different from a Erdős–Rényi RG. Most notably, these networks are characterized by a large cluster coefficient, $C = 0.59$, which is a purely geometric quantity independent of both node density and $\langle k\rangle$ [15, 17]. Furthermore, it has been shown numerically that the critical connectivity in these networks is at $\langle k\rangle = 4.52$ [27], which is much higher than the well-known $\langle k\rangle = 1$ value in RG.

2.2. Medium access control (MAC)

In WiFi networks access to the available frequency channels is controlled by a coordination mechanism called the MAC [30]. The function of the MAC is to ensure interference-free wireless transmissions of data packets in the network. This is achieved by scheduling in time the transmissions of nearby devices in such a way that devices whose radio transmissions may interfere with each other do not get access to the wireless channel at the same time. The presence of the MAC introduces novel spatio-temporal correlations in the dynamics of data communications in these networks which are absent in Internet communications.

The MAC protocol used by WiFi-based wireless devices follows the IEEE 802.11 standard [30], which specifies a set of rules that enable nearby devices to coordinate their transmissions in a distributed manner. The IEEE 802.11 MAC is a highly complex protocol and we do not attempt to fully model this protocol. Instead we focus on the most relevant aspect of this protocol, the so-called listen-before-talk (LBT) rule. This rule dictates that each device should check the occupancy of the wireless medium before starting a data transmission and refrain from transmitting if it senses that the medium is busy. The precise implementation of the LBT algorithm will be discussed in section 2.4.

2.3. Worm propagation model

Worms are stand-alone computer viruses which use networks for their spreading among computing devices. Consequently, computer worms can propagate automatically from device to device, in contrast to other types of virus which require some form of user involvement for their spreading.

Several previous studies have analysed and modelled the propagation of computer worms on the Internet. Most contemporary Internet worms work as follows [4]. When a computer worm is fired into the Internet, it scans the Internet protocol (IP) addresses and sends a probe to infect the corresponding machines. When a vulnerable machine becomes infected by such a probe, it begins running the worm and tries to infect other machines. A patch, which repairs the security holes of the machine, is used to defend against worms. When an infected or vulnerable machine is patched against a worm, it becomes immune to that worm. There are several different scanning mechanisms that worms deploy. Two main mechanisms are random scanning and local subnet scanning. In random scanning an infected computer scans the entire IP address space and selects its targets randomly from this space. In local scanning the worm scans the nearby targets (e.g. machines on the same subnet) with a higher probability. Many recent worms, such as Code Red v2 have used localized scanning.

The above mechanisms require that both the infected and the vulnerable nodes are connected to the Internet and rely on the IP routing mechanism for worm delivery. However, it is well-known that point-to-point routing of data packets in wireless ad hoc networks could be problematic due to the highly dynamic nature of these networks. A much more robust mechanism for disseminating packets in such networks is by multihop forwarding in which a packet propagates in the network by broadcast radio transmissions from device to device, without the need for any routing mechanism or Internet connectivity. This mechanism shows interesting analogies with the way airborne diseases spread in populations and has been exploited in a recent worm attack on Bluetooth-enabled smartphones [8]. We assume therefore that worms targeting these networks will utilize multihop broadcasts as their primary method of propagation. With respect to an attacking worm, we assume nodes in the network to be in one of the following three states: vulnerable, infected, or immune. Infected nodes try to transmit the worm to their neighbours at every possible opportunity. Vulnerable nodes can become infected at a rate λ when they receive a transmission containing a copy of the worm from an infected neighbour. Finally, infected nodes get patched and become immune to the worm at a rate δ. We denote by $S(t)$, $I(t)$ and $R(t)$ the population of vulnerable, infected and immune nodes, respectively.

2.4. Implementation

In our simulations we have implemented the above model of worm spreading in wireless ad hoc networks in the following way. At each timestep of simulations we create a randomly ordered list of the infected nodes in the network at that timestep. The first node on the list then gets access to the wireless channel and is allowed to transmit the worm. All other infected nodes that are within the transmission range of this node are eliminated from the list as their transmission may cause interference to that node, and is therefore blocked by the LBT rule. This procedure is repeated for the remaining nodes until the list is reduced to a set of non-interfering infected nodes which can transmit the worm at that same timestep.

Subsequently, all infected nodes which are on the above list go through a broadcast round in which they transmit the worm to their neighbours. Finally, all infected nodes (i.e. both those who were able to transmit the worm and those whose transmissions were blocked by the MAC protocol) go through a patching round in which they may become immune with probability δ.

3. Simulation studies

We simulated the propagation of worms in wireless ad hoc networks comprising N devices spread in a $L^2 = 1000 \times 1000\,\mathrm{m}^2$ area. The transmission range of all devices was set at 50 m, which is somewhere between the typical minimum (30 m) and maximum (100 m) range of the WiFi systems. In order to investigate the impact of device density we performed our simulations for a range of densities, corresponding to $N = 4000$, 6000, 8000, 10 000 and 20 000.

For a given density, nodes were distributed randomly and uniformly in the simulation cell. The resulting RGG networks were constructed following the prescription of section 2.1, and periodic boundary conditions were used in order to reduce finite-size effects. We verified numerically that all the networks considered were connected, and their degree distributions were well-described by the Poisson distribution:

$$P(k) = \mathrm{e}^{-\langle k\rangle}\frac{\langle k\rangle^k}{k!}, \tag{4}$$

with the average degree,$\langle k\rangle$, given by:

$$\langle k\rangle = \pi r_t^2 \rho, \tag{5}$$

where $\rho = N/L^2$ is the device density.

The spreading dynamics was simulated on top of the above networks using Monte Carlo simulations. Each Monte Carlo run starts by infecting a single randomly chosen node and proceeds following the rules described in sections 2.3 and 2.4 until the epidemic dies out (i.e. no infected node is left in the network). We typically average our results over 500 Monte Carlo runs. Furthermore, the results were also averaged over simulations starting from at least five different initial infected seeds. Since the timescale of the epidemic spreading depends only on the ratio λ/δ, rather than λ and δ separately, without the loss of generality we set the patching rate at $\delta = 1$ and performed our simulations for a range of values of the infection rate, λ.

In order to investigate the impact of the MAC on worm epidemics all simulations were performed both in the presence and in the absence of this mechanism. The latter case corresponds to an idealised scenario where nearby devices can communicate with each other without causing harmful interference, for example by using non-overlapping frequency channels[1], and maps the dynamics of worm spreading on to the standard susceptible-infected-removed (SIR) epidemic model. Finally, as a point of reference, we also performed simulation studies of the SIR model on a set of Erdős–Rényi RGs which were constructed such that their degree distribution virtually coincided with that of our RGG networks. In the following we shall refer to our full simulations as RGG + MAC while simulations in the absence of MAC will be labelled as RGG and those performed on random graphs as RG. For future reference we note that the SIR epidemic on RGs roughly mimics the spread of Internet worms via random scanning, and is well-described by the mean-field theory.

3.1. Prevalence and epidemic threshold

A key quantity in the study of epidemics in networks is the epidemic prevalence. For the SIR-type epidemics this quantity is defined as $R_\infty = \lim_{t\to\infty} R(t)/N$ [31]. In figure 1 prevalence as

[1] This might be the case, for example, in worm attacks on Bluetooth networks.

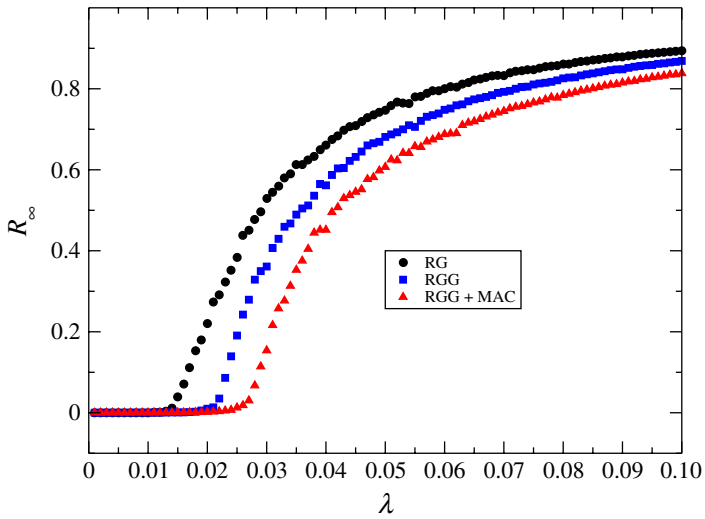

Figure 1. The epidemic prevalence, R_∞, is shown as a function of the infection rate λ for a wireless ad hoc network consisting of $N = 10\,000$ nodes, both in the absence and presence of the MAC mechanism. Also shown is the result for a RG network with the same number of nodes and the same degree distribution as the wireless ad hoc network.

a function of λ is shown as obtained from our simulations of, respectively, RG, RGG and RGG + MAC networks comprising $N = 10\,000$ nodes. It can be seen that in all these networks R_∞ exhibits a critical threshold λ_c below which a worm cannot spread in the network and above which it infects a finite fraction of the nodes. However, the epidemic threshold corresponding to RGG is at a considerably higher value than that of RG, despite the fact that the degree distributions of these two networks are identical. Furthermore, it can be seen that the inclusion of the MAC mechanism results in an increase in the value of the epidemic threshold in RGG, shifting the position of λ_c even further away from the RG value. Our computed epidemic thresholds for the above networks are $\lambda = 0.0140, 0.0210$ and 0.0265 for RG, RGG and RGG + MAC, respectively. The mean-field theory, which in the infinite system size limit becomes exact for the RG network, predicts an epidemic threshold at $\lambda_c = 1/\langle k \rangle$ [31, 32], yielding $\lambda_c = 0.0127$ for the above networks. This is in good agreement with our Monte Carlo result for the RG network, indicating that the above differences between λ_c in RG, RGG and RGG + MAC are not due to finite-size effects (or statistical fluctuations) but are caused by a combination of topological and dynamic correlations in our wireless networks, which are absent in RG.

Qualitatively, we can understand the above results by noting that due to spatial ordering in RGGs, the epidemic state of a node in a RGG is strongly correlated to the state of its neighbours. These correlations reduce the so-called reproductive rate of the epidemic, the average number of new infections that can be produced by an infective node, below the value predicted by the mean-field approximation, hence increasing λ_c above the mean-field value. The presence of the MAC introduces additional temporal correlations between the transmission times of adjacent infective nodes which further reduce the reproductive rate, hence further increasing λ_c above the mean-field value. It can be seen from figure 1 that this latter mechanism not only affects λ_c but also results in a significant reduction in the epidemic prevalence.

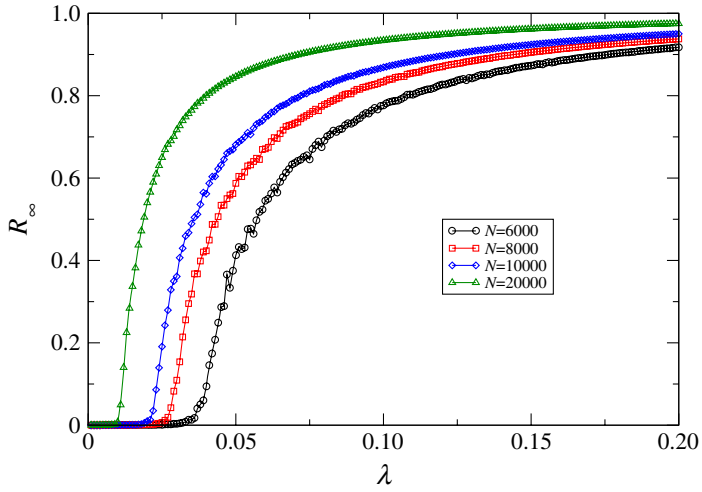

Figure 2. The epidemic prevalence, R_∞, as a function of the infection rate λ is shown for wireless ad hoc networks comprising $N = 6000, 8000, 10\,000$ and $20\,000$ nodes, respectively. Results are shown for simulations performed in the absence of the MAC mechanism.

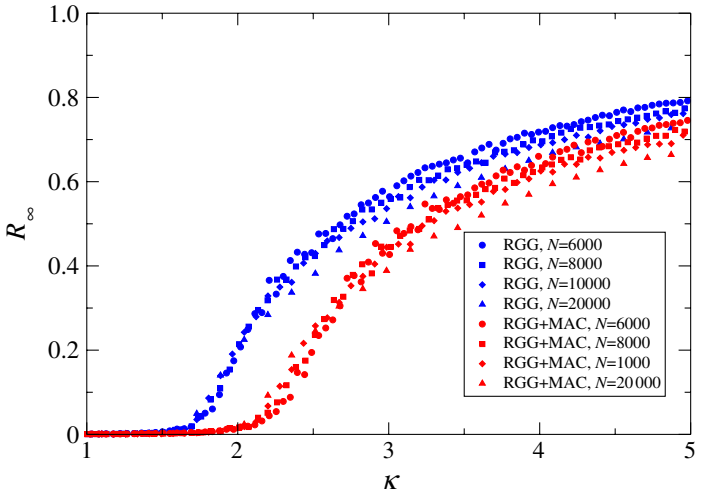

Figure 3. Collapse plots of R_∞ versus $\kappa = \lambda\langle k\rangle$ are shown for wireless ad hoc networks comprising $N = 6000, 8000, 10\,000$ and $20\,000$ nodes, both in the presence and absence of the MAC mechanism.

Next we investigate the impact of node density, ρ, on the behaviour of epidemic prevalence in our networks. In figure 2, we plot R_∞ as function of λ for different device densities. Results are shown only for RGG but they show a similar behaviour for RGG + MAC. It can be seen that for all densities considered the revalence shows a critical behaviour. However, the position of λ_c decreases monotonically with increasing density, i.e. the worm epidemic is more successful in invading the network when the density of devices is high and less so when density is low. In order to better understand the density-dependent behaviour of R_∞ we plot in figure 3 this quantity as function of $\kappa = \lambda\langle k\rangle = \lambda\pi\rho r_t^2$. It can be seen that for RGG there is a good collapse of curves

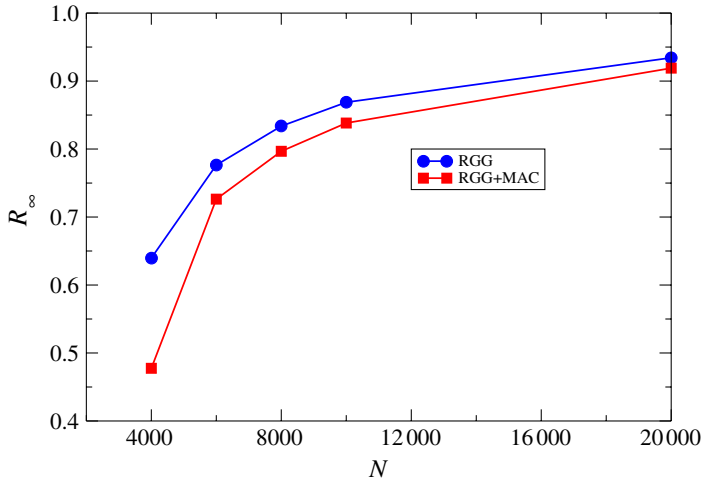

Figure 4. The epidemic prevalence in a wireless ad hoc network is plotted as a function of the number of devices in the network. Results of simulations performed in the absence (circles) and presence of the MAC (squares) are shown.

in an extended region around the threshold. This indicates that in this region the prevalence of the SIR model on RGG is well-described by the scaling relation $R_\infty(\lambda, \rho) = f(\kappa)$ (for RGG + MAC this scaling holds only approximately). In particular, we find that the epidemic threshold itself can be written as:

$$\lambda_c = \frac{\kappa_c}{\langle k \rangle} = \frac{\kappa_c}{\pi \rho r_t^2}, \tag{6}$$

with $\kappa_c = 1.50$, a correction to the mean-field model resulting from spatial correlations in RGG. Since the cluster coefficient, C, is a measure of correlations in a network, we note that the value of κ is in fact very close to $1/C$ indicating that the departure from the mean-field model is possibly controlled by this quantity.

Next, we investigate the dependence of the epidemic prevalence on device density. In figure 4 this quantity is plotted as a function of N and for $\lambda = 0.1$, both in the presence of MAC and when this mechanism is switched off. It can be seen that in both cases R_∞ increases monotonically with increasing node density. Furthermore, for all values of N the curve corresponding to RGG+MAC lies below that of RGG. However, the gap between the two curves decreases as N is increased, indicating that the impact of MAC on R_∞ becomes less significant at high densities.

3.2. Spreading dynamics

Finally, we discuss the propagation dynamics of worms in our networks. Figure 5 displays, as an example, time evolution of the total fraction of infected nodes, $I(t)/N$, in the $N = 10\,000$ node network and for $\lambda = 0.1$. For comparison, we have also plotted the result obtained for the corresponding RG network. As can be seen from figure 5, worm spreading on the RGG network takes place at a much slower pace than on the RG network. In particular, the initial growth of the epidemic on RGG is much slower than the exponential growth seen for RG, which is a hallmark of mean-field models [33] and is also observed in epidemics in the Internet [2].

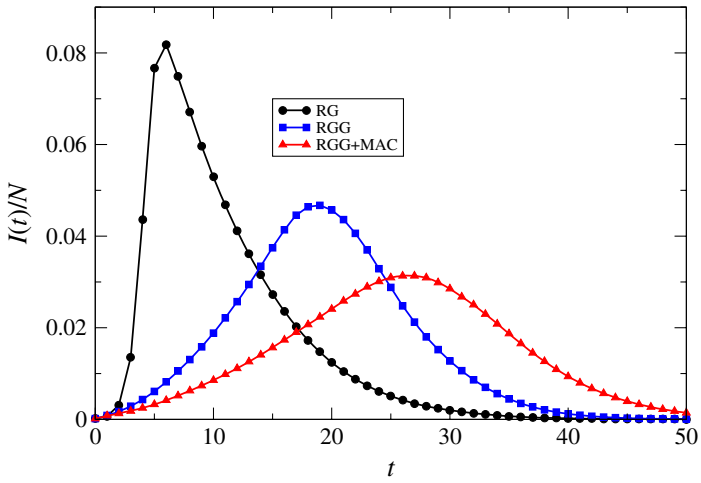

Figure 5. Time evolution of the fraction of infective devices, $I(t)/N$, is shown for networks consisting of $N = 10\,000$ nodes. Results of simulations are shown both in the absence (squares) and presence (triangles) of MAC. Also shown are the results for the corresponding RG network (circles).

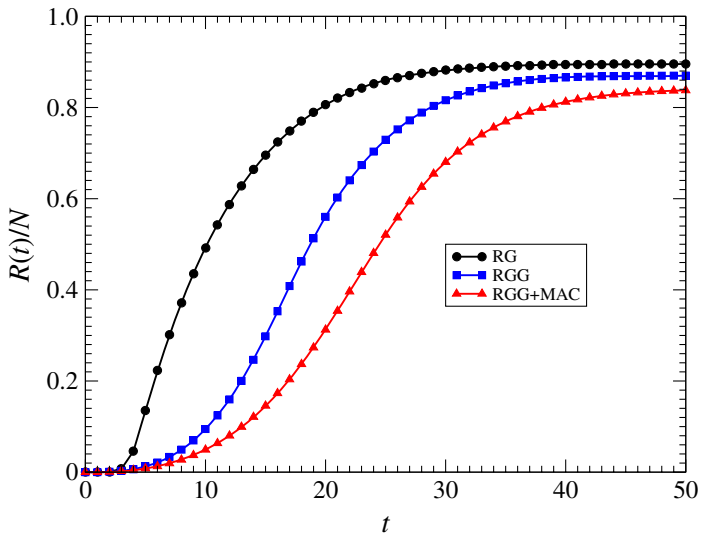

Figure 6. Time evolution of the fraction of immunized devices, $R(t)/N$, is shown for the same networks as in figure 5.

The above slow growth of the epidemic on the RGG is a purely topological effect, which we attribute to a combination of spatial correlations and high clustering in this network. As can be seen from figure 5 switching on the MAC protocol in RGG slows down the epidemic on this network even further. This effect, which we call *self-throttling*, is caused by temporal correlations in the spreading dynamics introduced by the MAC and has also been observed in a recent study of IP-based worm spreading in mobile ad hoc networks [7]. It results because adjacent infective devices compete with each other in accessing the shared wireless medium, hence effectively blocking each other's broadcasts and slowing down the overall progress of the epidemic. In figure 6, we display our result for $R(t)/N$ in the $N = 10\,000$ networks, which further

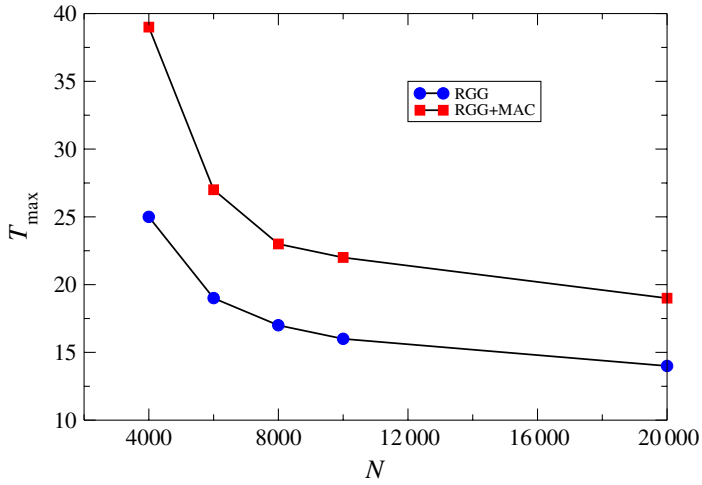

Figure 7. The position of the epidemic peak, T_{max}, in RGG networks is plotted as function of N. Results are shown when the MAC is switched off (circles) and when it is switched on (squares).

demonstrates the great impact of spatial and temporal correlations on the spreading process in our wireless networks.

Next we discuss the impact of device density on the speed of worm propagation. As an indicator of the speed we use the position of the peak in $I(t)/N$, which we call T_{max}. This quantity is plotted in figure 7 as a function of N, both in the absence and presence of MAC. It can be seen that both curves show a monotonic decrease with increasing node density. Furthermore, we see that the self-throttling mechanism is most effective in slowing down the epidemic at the lowest density, where we observe a $\sim$40% increase in T_{max} when MAC is switched on. As density increases the gap between the two curves becomes initially smaller before settling down at higher densities.

4. Conclusions

In this paper, we introduced a model for the propagation of a new class of computer worms which specifically target wireless computing devices. Using extensive Monte Carlo simulations we investigated the epidemic spreading of such worms in WiFi-based wireless ad hoc networks. We incorporated the spatial topology of these networks via a RGG model, and also took into account the impact of the MAC on wireless data communications in these networks.

Our studies show that worm epidemics in wireless ad hoc networks are greatly different from the previously studied epidemics in the Internet. The epidemic threshold was found to be density-dependent and for all densities considered significantly higher than the value predicted by the mean-field theory. Furthermore, the initial growth of the epidemic was found to be significantly slower than the exponential growth observed in Internet epidemics and predicted by the mean-field theory. We showed that these differences were due to a combination of spatial and temporal correlations which are inherent to wireless data networks. Our study also revealed the presence of a self-throttling mechanism which results from a competition between adjacent infected devices

for access to the shared wireless medium. This mechanism greatly reduces the speed of worm propagation and the risk of large-scale worm epidemics in these networks.

An understanding of the propagation characteristics of worm attacks on wireless networks is of great importance for the design of effective detection and prevention strategies for these networks. The work presented in this paper is a first step in this direction and, we hope, will inspire future empirical and theoretical investigations. From the perspective of complex network theory, our work presents an extensive study of epidemic spreading in RGG, and highlights the important role that spatial correlations play in dynamic processes on these and other spatial networks.

Acknowledgments

MN acknowledges support from the Royal Society through an Industry Fellowship and thanks the Centre for Computational Science at UCL for hospitality.

References

[1] Stantiford S, Paxton V and Weaver N 2000 *Proc. 11th USENIX Security Symp. (Security '02)*
[2] Chen T M and Robert J-M 2004 *IEEE Comp.* 48–53
[3] Pastor-Satorras R and Vespignani A 2004 *Evolution and Structure of the Internet: A Statistical Physics Approach* (Cambridge: Cambridge University Press)
[4] Szor P 2006 *The Art of Computer Virus Research and Defense* (Crawfordsville, IN: Symantec)
[5] Moore D and Shannon C 2003 Code-Red: a case study on the spread of victims of Internet worms *Proc. 2002 SIGCOMM Internet Measurement Workshop* (*Marseilles, France*) pp 273–48
[6] Levitt N 2005 *IEEE Comp.* **38** 20–23
Dagon D, Martin T and Starner T 2004 *IEEE Pervasive Comput.* **3** 11–15
[7] Cole R G 2004 *Army Science Conf. 2004 (Orlando, FL)*
[8] Hypponen M 2006 *Sci. Am.* November pp 70–77
[9] Pastor-Satorras R and Vespignani A 2001 *Phys. Rev. Lett.* **86** 3200
[10] Newman M E J, Forrest S and Balthrop J 2002 *Phys. Rev.* E **66** 035101
[11] Goldenberg J, Shavitt Y, Shir E and Solomon S 2005 *Nature Phys.* **1** 184–8
[12] Balthrop J, Forrest S, Newman M E and Williamson M M 2004 *Science* **304** 527–9
[13] Nekovee M 2006 *Proc. IEEE VTC Spring 2006 (Melbourne, Australia)*
[14] Hekmat R 2006 *Adhoc Networks: Fundamental Properties and Network Topologies* (Berlin: Springer)
[15] Glauche I, Krause W, Sollacher R and Geiner M 2002 *Physica* A **325** 577–600
[16] Kraus W, Glauche I, Sollacher R and Geiner M 2004 *Physica* A **338** 633–58
[17] Glauche I, Krause W, Sollacher R and Geiner M 2004 *Physica* A **341** 677–701
[18] Krause W, Scholz J and Geiner M 2006 *Physica* A **361** 707–23
[19] Albert R and Barabási A-L 2002 *Rev. Mod. Phys.* **74** 47
[20] Dorogovtsev S N and Mendes J F F 2002 *Adv. Phys.* **51** 1079–187
[21] Newman M E J 2003 *SIAM Rev.* **45** 167
[22] Boccaletti S, Latora V, Moreno Y, Chavez M and Hwang D-U 2006 *Phys. Rep.* **424** 175
[23] Heramnn C, Barthélemy M and Provero P 2003 *Phys. Rev.* E **68** 026128
[24] ben-Avraham D, Rozenfeld A F, Cohen R and Havlin S 2003 *Physica* A **330** 107–16
[25] Rappaport T 2000 *Wireless Communications, Principle and Parctice* (Englewood Cliffs, NJ: Prentice-Hall)
[26] Penrose M 2003 *Random Geometric Graphs* (Oxford: Oxford University Press)

[27] Dall J and Christensen M 2002 *Phys. Rev.* E **66** 016121
[28] Sosperda Alfonso R 2005 On random geometric graphs: structure and epidemics *MPhil Thesis* ICTP
[29] Bollobas B 1998 *Modern Graph Theory* (New York: Springer)
[30] Gast M S 2005 *802.11 Wireless Networks* 2nd edn (Sebastopol, CA: O'Reily)
Stalling W 2005 *Wireless Communications Networks* (Englewood Cliffs, NJ: Prentice Hall)
[31] Moreno Y, Pastor-Satorras R and Vespignani A 2002 *Eur. Phys. J.* B **63** 521
[32] Boguna M, Pastor-Satorras R and Vespignani A 2003 *Lecture Notes in Physics* **625** 127–47
[33] Bathélemy M, Barrat A, Pastor-Satoras R and Vespignani A 2004 *Phys. Rev. Lett.* **92** 178701