Modeling Framework for the Study and Analysis of Mobile Attack Propagation in Wireless Ad-Hoc Networks

Vasileios Karyotis, Symeon Papavassiliou and Basil Maglaris

Network Management & Optimal Design Lab (NETMODE)
Dept. of Electrical and Computer Engineering
National Technical University of Athens, Zografou, Greece
vassilis@netmode.ntua.gr, {papavass|maglaris}@mail.ntua.gr

Abstract - **Independent-operating attacks in modern communication networks have become increasingly popular, affecting significantly the performance of these networks and causing major systems to fail. In this paper, we introduce and design a modeling framework that allows for the study and analysis of mobile attack propagation in wireless ad-hoc networks. Specifically, we study probabilistically the propagation of a worm in a wireless ad-hoc network, in which an energy-constrained malicious node can move freely in the deployment region of the network. The choice of a statistical approach of the problem is motivated by the dynamic characteristics of the ad-hoc topology and the stochastic nature of the worm propagation. Through modeling and simulation, we studied and evaluated the impact of various parameters associated with the operational characteristics of the mobile attack node – such as transmission radius, mobility, energy – on an outbreak spreading and the evolution of the network, and obtained an in-depth understanding of the importance of these parameters both from the network's and the attacker's perspectives.**

1. Introduction

One of the most important issues in modern computer and telecommunication networks is the vulnerability of network hosts to several minor or severe threats. Modern network threats can be classified into two major categories: those that are host-dependent and those that are able to operate independently. The first type works on a local host and essentially cannot affect other connected machines. On the contrary, the second type is able to migrate from a host to another, spreading throughout the entire network.

In wireless ad-hoc networks, where nodes tend to collaborate with each other in order to provide end-to-end multi-hop communications, and at the same time present several resource limitations, the problem of threat propagation/spreading poses additional issues and challenges. In these networking environments, the problem is further complicated by the fact that they do not present fixed network infrastructure or administrative support, while the time-varying nature of the wireless domains in combination to the power limitations and the effects of mobility, make the corresponding topology vary dynamically as time evolves.

Obtaining an in-depth understanding of the way an outbreak spreads in a wireless ad-hoc network can be proven extremely useful in choosing the proper countermeasures. Similarly, from the attacker's perspective, prior knowledge of the specific model that an infection follows during the spreading phase can make an attack more efficient and harmful.

The objective of this paper is to introduce and design a modeling framework, which would allow for the study and analysis of mobile attack propagation in wireless ad-hoc networks. Specifically, we study probabilistically the propagation of a worm in a wireless ad-hoc network, in which a malicious node can move freely in the deployment region of the network. The choice of a statistical approach of the problem is motivated by the dynamic characteristics of the ad-hoc topology and the stochastic nature of the worm propagation.

The rest of the paper is organized as follows. In section 2 we describe some related work, while in section 3 the system model and corresponding assumptions are presented. In section 4 we provide the detailed description of the attack propagation modeling approach, while section 5 contains some numerical results and relevant discussions. Finally, section 6 concludes the paper.

2. Related Work

The propagation of worm programs in computer networks is similar to the propagation of viruses infecting members of a closed population. Some of the elements of the set are infected, and since every member has established interactions with a subset of the members of the set, an infection can be propagated through such existing interactions. At the same time, there is a possibility that an element can recover from the infection.

The behavior of such systems has been studied extensively in the cases of biological organisms, and it is only recently that similar studies have been performed in the field of computer networks [1], [2]. In the case of biological individuals, the emphasis has been placed on the field of *epidemics* [3]. The basic tool used for the analysis of epidemics problems is differential equations. The number of infected nodes is the unknown variable of the problem and the objective is to formulate an ordinary differential equation containing the unknown parameter. The solution of this equation yields the number of infected nodes of a network as a function of time [3], [4], [5]. However, this approach reveals only the pattern followed by the

percentage of infected nodes, and it does not reveal the parameters influencing the observed trend. The next step is to proceed with a precautionary immunization of several nodes, expecting to block the propagation of the infection in several critical parts of the network. It should be noted however that the immunization is usually random and no special characteristics of the specific topology are taken into account in choosing the immunized subset of nodes.

Another approach for modeling the spread of infections, deals mainly with the propagation of worm programs in computer networks [5], [6]. The special operation of such entities (e.g. port scanning, ip domain attacks) is exploited in modeling and analyzing such threats. The basic study tool in such cases is simulation and the countermeasures are again precautionary immunizations.

A more systematic and theoretic way to deal with worm propagation contains probabilistic-based methodologies, where the corresponding processes of infection and recovery are modeled on a statistical basis. For instance, for each node there exists a probability to become infected through a communication link and similarly one for recovery, once infected. The corresponding patterns of infection and recovery are assumed to follow different stochastic patterns [7]. With respect to the previous model, analytical tools can be used to predict and control the behavior of the system dynamically and accurately.

Most of the above approaches mainly refer to wired networks with static topologies. On the other hand, our study aims at developing a systematic framework that allows for the modeling and study of attack propagation in wireless ad-hoc networks and incorporates the impact of attack parameters in the probabilistic method of worm propagation.

3. System Model and Assumptions

In general, at a given point in time, depending on the various nodes' positions, the wireless channel conditions, the transmitter and receiver coverage patterns, the transmission power and co-channel interference levels, the wireless connectivity between network nodes can be represented in the form of random, multihop graph. In a wireless network, a node can have connectivity with multiple nodes in a single physical radio link. For our purposes a node A can consider another node B to be adjacent ("neighbor") if there is link-level connectivity between A and B and A receives messages from B reliably. Accordingly, we can map a physical broadcast link connecting multiple nodes into multiple point-to-point bidirectional links defined for these nodes.

Throughout our study, we consider a system that consists of a set of wireless nodes, each with a fixed transmission radius R. The nodes are uniformly and randomly deployed over the network region. The deployment region is a two dimensional space of specific shape (square, circular, hexagon, etc.). Furthermore, in order to obtain a better understanding of the mobile attack propagation model the nodes of the network are assumed static. However, we consider that a mobile malicious node, wanders around the network, therefore infecting the rest of the nodes. This affects the communication links between the attacking node and the rest of the network. The nodes of the underlying network can also infect their neighbors once they become infected by the attacker or a neighbor of their own.

As the wireless channel varies significantly over time, its variations can be statistically described as small-scale and large-scale variations. In our case, we average over any large-scale variations (modeled by a lognormal shadowing model [8]), and discard any small-scale variations (modeled by a Rayleigh distribution [8]). Thus, the received signal averaged over the large-scale variations, has an inverse power dependence of the distance from the transmitting node, where the exponent is the path loss constant (usually determined between 2 and 4 through field measurements). Consequently, the neighbors of a node are completely determined by its transmission radius. All the nodes lying inside the disk centered at a specific node X with radius equal to its transmission radius are assumed to be the neighbors of node X.

4. Attack Propagation Modelling

The probabilistic formulation of the problem is based on the link-probability of infection. There exists a specific probability that a node having a communication link with an infected node will become infected from it[1]. Thus, we assume a node can become infected even if it is already infected, in which case the recovery process of the node is reset. A specific node usually has more than one neighbor, and therefore if a subset of them is infected, the node can become infected from any of those links. The number of infections that a node receives from a single link is a random variable, where we assume that it follows Poisson distribution. This means, that the infection inter-arrival times on a communication link are exponentially distributed.

With respect to the recovery process of a node, since not all the users of the nodes are able to deal with the infection identically, this process is of stochastic nature as well. Throughout our study, we assume that the recovery process follows Poisson distribution, so that time intervals between successive recoveries are independent and exponentially distributed. The node model described above can be mapped to that of an M/M/1 queue. An infection is mapped to an arrival, which needs service, and the recovery is mapped to the service discipline itself, while both arrivals and services are assumed independent and exponentially distributed. It should be noted that this formulation holds true for the whole duration of the attacker's lifetime. As mentioned before the attacker (e.g. malicious node), is allowed to move throughout the network, infecting the rest of the nodes, until its energy is exhausted.

[1] Without loss of generality, we omit the details of the specific way the infection occurs, and focus on the infection event itself, as taking place with a positive probability.

Assuming that the state of each node is binary (infected, non-infected), the system state is given by a binary vector, where the rows correspond to the network nodes and the value of each vector component indicates infection or non-infection. Assuming a network with N nodes the state space will have 2^N possible states. As discussed earlier, there are two types of events: infections and recoveries. We can easily conclude that the time intervals between successive events for a node are exponentially distributed with rate the sum of the partial rates of infections and recovery.

Let us consider that there are N nodes in the network and one attacker. If m denotes the number of nodes that are non-infected at a given instant, then there are $N-m$ infected nodes (excluding the attacker). Supposing an event has just taken place, with the above assumptions for the infection and recovery processes, the time interval for the next event is exponentially distributed with rate:

$$\sum_{i=1}^{m} k_i \lambda_i + \sum_{i=m+1}^{N} \mu_i \qquad (1)$$

where k_i is the number of infected neighbors of node i, μ_i denotes its recovery rate and λ_i denotes its link infection rate. The summation index spans the sequence of the network nodes where, without loss of generality, we assumed that the non-infected nodes are the first m in the sequence. The infection and recovery processes are all assumed independent of each other.

The lifetime of a malicious node depends mainly on its available energy and transmission radius. In a wireless ad-hoc network, for a fixed time interval the energy consumption is much higher for a node with large radius rather than a node with a small radius. The energy depletion discipline is modeled through an iterative process as follows:

$$E_{avail} = E_{prev} - A\left(t_{sp} r^a\right) E_{step} \qquad (2)$$

where E_{avail} is the updated energy inventory, E_{prev} is the inventory before the update, E_{step} denotes a depletion step value, r is the transmission radius of the attacker, t_{sp} denotes the time interval since the last energy update, a is the path loss constant and A is a normalization constant, used to represent all constant factors of the depletion model. Equation (2), essentially relates the depletion of the available energy with the transmission radius and the system time (current lifetime) of the malicious node.

5. Numerical Results and Discussion

In this section, based on the developed model and framework, we study the impact of various parameters associated with the operational characteristics of a mobile attack node on the model behavior, the attack propagation, and the evolution of the network. This is achieved via modeling and simulation. Specifically, we aim at evaluating the influence of the attacker's radius on the propagation of the threat in conjunction with the node's energy consumption and lifetime. We also study the impact of the attacker's mobility on the evolution of the network and the spreading of the threat.

Among the objectives of our research work is to identify the various trade-offs that these parameters present, in order to provide guidelines to choose the appropriate values of these design parameters that achieve the desired performance, both from the network and the attacker's point of view.

It should be noted that the performance results presented in this section constitute a preliminary subset of results of our performance evaluation process. A more in-depth and systematic analysis of the proposed model is still in progress in order to obtain a more detailed understanding of the way an outbreak spreads in a wireless ad-hoc network and evaluate the impact of different mobile attack strategies with respect to a complete set of operational and performance metrics and under various static and mobile scenarios.

5.1. Simulation Model

In the following, we consider a wireless ad-hoc network where the nodes are uniformly distributed in a square area of $1000m \times 1000m$, and each node has a fixed limited transmission range $R = 200m$. This radius determines the connectedness of the underlying network topology. In order to study the impact of the attacker's radius on the attack propagation we assume that the radius of the malicious node may vary among different simulation instances. Furthermore, for simplicity in the presentation of the results, we also assume that all nodes have the same link-infection and recovery rates (i.e. $\lambda = 0.1 \, or \, 0.3$ and $\mu = 0.9$ respectively).

The attacker is assumed to move throughout the network according to a random mobility model with zero stop time [9]. The speed of the attacker is randomly chosen in the interval $[0, v_{\max}]$ and its direction is uniformly distributed within interval $[0, \theta_{\max})$. Throughout our study we consider two cases of $\theta_{\max}$, namely $\theta_{\max} = 2\pi$ and $\theta_{\max} = \pi$. In the following, we refer to the first one as random movement, and to the second one as directional movement. Occasionally, the node selects again a speed and direction, independently of its previous choices.

Due to the finiteness of the deployment region, it is possible that the attacker will reach the boundary of the region. To deal with this event, we assume that the region folds like a torus, so that if a node crosses a boundary, it reenters the region from the opposite boundary with respect to the center of the region. The normalization constant A of the energy depletion model presented in section 5 (i.e. relation (2)), is chosen such that the depletion rate ensures sufficient simulation time for the system to reach its steady state. The initial energy reserve is set to $E = 150$ energy units (eu), the step depletion value is $E_{step} = 0.1eu$, while the path loss constant a was assumed $a = 2.5$.

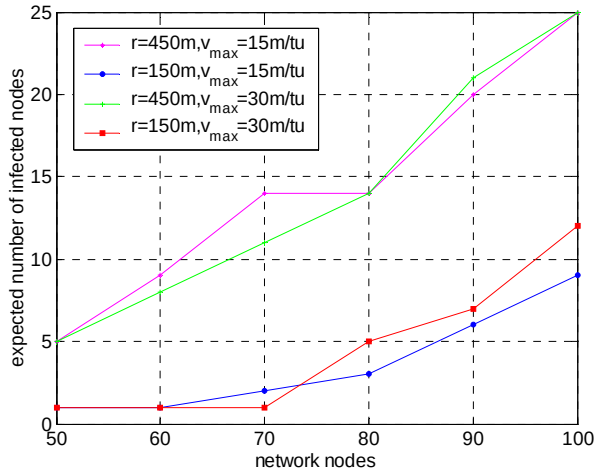

Figure 1 - Expected number of infected nodes for random movement

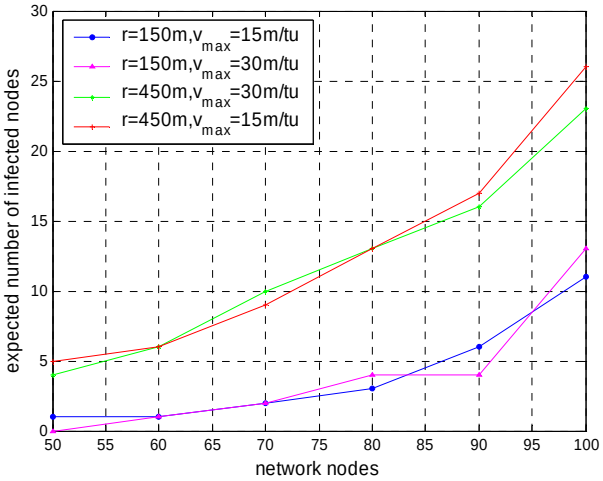

Figure 2 - Expected number of infected nodes for directional movement

5.2. Numerical Results and Discussion

Throughout our numerical study, multiple network topologies and different values of the operational parameters of the mobile malicious node were used. More specifically the network size varied from 15 nodes to 100 nodes, while the system was studied for two sets of values of the attacker's transmission radius, i.e $r = 150m/450m$ and $r = 200m/300m$. In addition, with respect to the mobility of the malicious node different maximum speeds (expressed in meters per time unit *(m/tu)*) were considered and different cases were examined, including random movement and directional movement.

In Figure 1 the expected number of infected nodes is presented as a function of the network size (i.e. number of nodes) for four different radius-speed combinations, under the assumption of random movement for the malicious node. Similarly, Figure 2 presents the corresponding results for the case of directional movement, where the mobile threat is now constrained in the movement direction. Observing Figure 1 and Figure 2, we notice that the trends of the curves as well as the corresponding numerical results are quite similar. Specifically, from both the above figures, we can easily conclude that, as the network density increases (i.e. as the number of nodes increase), the influence of the transmission radius and the node's speed decreases. In such cases, the dominant factor in the propagation of the network attack is the underlying topology and the way that the infection is propagated from the other nodes of the network to their neighbors, while the impact of the movement of the attacker in this process is relatively insignificant. Similarly, for sparse topologies smaller transmission radius means fewer expected number of infected nodes. It should be noted here however that naturally, the lifetime of an attacker with larger radius is significantly smaller than a case with small radius.

The aforementioned remarks can be seen more clearly in the instants presented in Figure 3. The infection rate was chosen $\lambda=0.3$, the path loss constant $a = 4$ and $R = 300m$ thus increasing significantly the probability of infection for a network node.

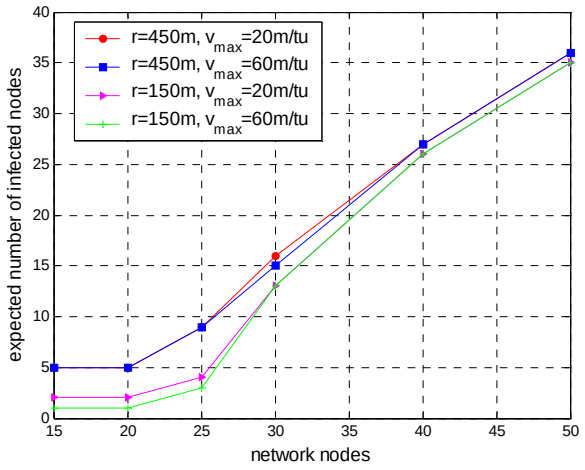

Figure 3 - Expected number of infected nodes for random movement ($\lambda=0.3$)

It can be seen from Figure 3, that for denser topologies the propagation is dominated by the underlying network, while in sparser ones, the mobile attacker plays a more critical role. Therefore, from an attacker's perspective, for sparse topologies it is more efficient to increase its transmission radius, to infect as many nodes as possible, and then rely on the propagation of the infection among them. On the other hand, since the impact of the mobility on the average number of infected nodes is very small for dense networks, it is more effective to reduce its power, and stay alive longer in the network, in order to re-infect the network in case of full recovery. We should note here that the energy depletion discipline used in our model is mainly based on the impact of transmission radius, since it is known that in wireless ad hoc networks the main part of energy consumption is due to communication (transmission and reception). However, it is part of our current research to use models that incorporate energy penalties due to mobility in the energy depletion rule and study the corresponding impact on the respective results.

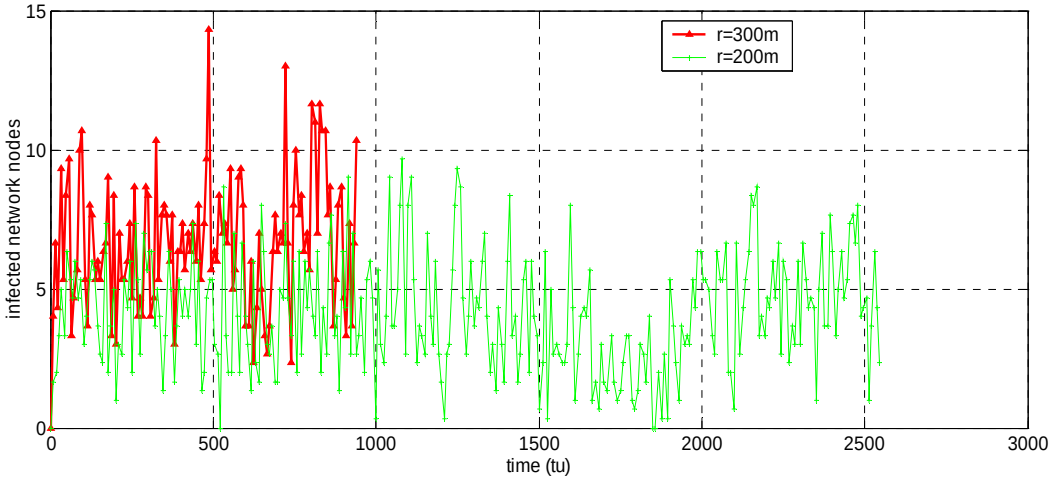

Figure 4 – Network evolution, random movement, N=75 nodes

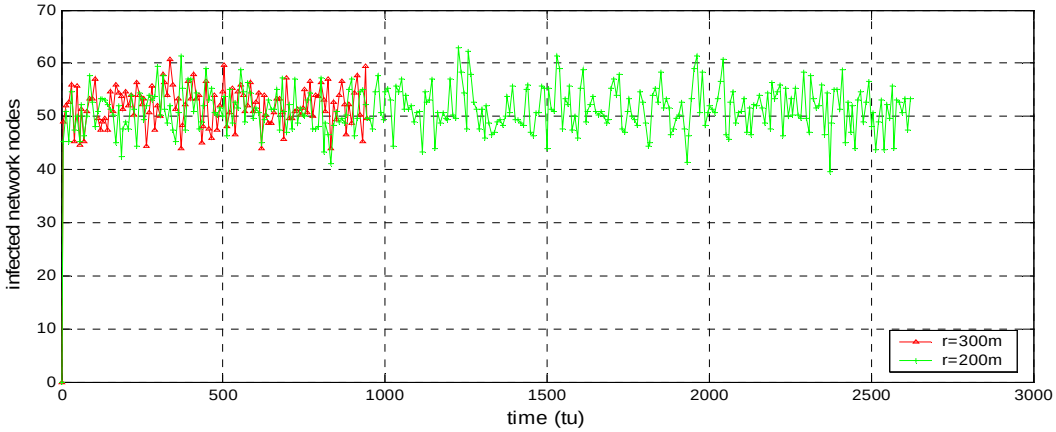

Figure 5 - Network evolution, random movement, N=100 nodes

In Figure 4 and Figure 5 we present the evolution of the number of infected nodes as the system evolves, for different topologies with respect to the network size (i.e dense and sparse topology). The horizontal axis is expressed in time units. The two curves in each figure correspond to different transmission ranges of the malicious attack node (i.e. $r = 200m$ and $r = 300m$). With respect to the sparser topology, as demonstrated in Figure 4, we observe that in the case of larger transmission radius, a greater number of nodes become infected initially, when compared against the case of smaller transmission radius. However, as the time and network evolves, both instants fluctuate around the mean value of the number of infected nodes, with the $r = 300m$ instant having slightly higher mean value, as mentioned before. In the case of a denser topology (Figure 5), similar patterns are observed as well, with the difference that eventually the mean value of the two instants is practically the same. However, as naturally expected and also observed from these figures, the attacker's lifetimes for the two scenarios differ significantly. It should be noted here that each scenario is simulated until the energy of the corresponding mobile attack node is exhausted. Therefore the point of the horizontal axis where each curve ends represents the lifetime of the mobile node in every case.

6. Concluding Remarks and Future Work

Worm propagation in computer networks has drawn much attention recently. While most of the previous work was mainly aimed at wired networks, our work emphasizes on the introduction and design of a probabilistic framework for the spreading of an active mobile worm in a wireless ad-hoc network, where the attacker is energy constrained.

Based on the proposed modeling framework, we studied the impact of various parameters associated with the operational characteristics of the mobile attack node – such as transmission radius, mobility, energy – on the attack propagation and the evolution of the network. The corresponding outcomes and observations, on one hand, can be used from the attacker in order to develop a more effective and harmful strategy. On the other hand, however, an in-depth understanding of the way an outbreak spreads in a wireless ad-hoc network can facilitate the choice of the proper countermeasures.

One of the recent approaches towards this direction for the case of wireless ad-hoc networks, are those that exploit the ability to control the topology of such networks. The basic idea behind such methods is that a node can adjust its transmission power to vary its

transmission range and consequently the connectivity with several neighbors. Thus, if there is side-information for a threat, a node can reduce its range to disconnect from potentially infected neighbors. Another way of altering the underlying topology to avoid malicious attacks is to allow various network nodes have mobility capabilities. A mobile host can take advantage of the side information to move away of areas of potential increased danger. Studying the impact of such techniques in the propagation of active threats in wireless ad-hoc networks, is part of our current and future research.

ACKNOWLEDGEMENT

This work was partially supported by Greek General Secretariat for Research and Technology of the Ministry of Development (PENED project 03ED840).

REFERENCES

[1] Ganesh A. Massoulie, L. Towsley D. "*The effect of network topology on the spread of epidemics*". In Proc. of 24th IEEE Conference on Computer Communications (IEEE INFOCOM 2005), Vol.II, pp.1455 – 1466, March 2005.

[2] S. Tanachaiwiwat, A. Helmy, "*VACCINE: War of the Worms in Wired and Wireless Networks*". USC Technical Report, July 2005, Los Angeles, USA.

[3] R. Pastor-Satorras and A. Vespignani. "*Epidemics and Immunization in Scale-Free Networks*". In Handbook of graphs and networks: from the genome to the Internet, editors S. Bornholdt and H. Schuster, pages 113-132, Berlin, 2002. Wiley-VCH.

[4] C.C. Zou, W. Gong, D. Towsley, "*Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense*". In the First ACM Workshop on Rapid Malcode (WORM), October 27, 2003, Washington, DC, USA.

[5] Z. Chen, L. Gao, K. Kwiat, "*Modeling the Spread of Active Worms*". In Proc. of 22nd IEEE Conference on Computer Communications (IEEE INFOCOM 2003), Vol.III, pp.1890-1900, April 2003.

[6] C.C. Zou, D. Towsley, W. Gong, "*Email virus propagation modeling and analysis*". Technical Report TR-CSE-03-04, University of Massachusetts, Amherst, MA, USA.

[7] V. A. Karyotis. "*A Base Case Study of the Worm Propagation Problem in the Framework of Topology Control in Wireless Ad-Hoc Networks*". Master's Thesis, August 2005, School of Engineering & Applied Sciences, University of Pennsylvania, Philadelphia, PA, USA.

[8] T. S. Rappaport, "*Wireless Communications*: *Principles and Practice*". Englewood Cliffs, NJ: Prentice-Hall, 1996, pp. 69–122, 139–196.

[9] C. Bettstetter, G. Resta, P. Santi, "*The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad-Hoc Networks*", IEEE Transactions on Mobile Computing, Vol. 2, No. 3, July-September 2003.