

# Analyzing the Spread of Active Worms over VANET\*

Syed A. Khayam and Hayder Radha

Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA

{khayamsy, radha}@egr.msu.edu

## ABSTRACT

This paper investigates the parameters governing the spread of active worms over VANET. To this end, we first define the average degree of a VANET node using freeway traffic parameters. The spread of a worm in congested and low-density traffic scenarios is modeled using a stochastic model of infectious disease. Analysis is provided for preemptive and interactive patching scenarios.

## Categories and Subject Descriptors

D.4.6 [Security and Protection]: Invasive software.

## General Terms

Security, Design, Reliability, Theory.

## Keywords

VANET, Computer worms, Stochastic modeling, Epidemiology.

## 1. INTRODUCTION

An active worm over VANET can, in addition to the well-known threats, pose a whole new class of traffic-related threats ranging from congestion to large-scale accidents. Design of secure VANET applications can benefit from a thorough understanding of the spread of computer worms over a typical VANET. In this paper, we investigate the parameters governing the spread of active worms over VANET. We define an *average effective distance* between two VANET vehicles using freeway traffic parameters and then use this distance to describe the behavior of a VANET link as a *log-normal shadow fading channel* [2]. The shadow fading channel model is employed to define the VANET topology as a *geometric random graph* and the average node degree of the graph is derived. We run the *stochastic Susceptible, Infected, Removed (SIR) epidemic model* [3] on the geometric random VANET graph. For both congested and low-density traffic scenarios, we derive expressions for the rate of worm spread as a function of the average degree of the graph and the rate at which VANET nodes are being patched. We analyze two cases of worm spread: 1) preemptive patching, where the number of patched VANET nodes remains constant; 2) interactive patching, where patching is performed during a worm outbreak.

## 2. VANET CHANNEL MODEL

The Fleetnet group defined the average effective distance between two vehicles as [4],

$$d_a = \frac{v_a \tau}{L} \quad (1)$$

where,  $v_a$  is the average velocity of vehicles;  $\tau$  is the average time headway between two vehicles; and  $L$  is the number of lanes in the freeway.

\* A full version of this paper is available in [1].

Given a receiver sensitivity,  $p_r \geq p_{r,th}$ , a link exists between two nodes if the attenuation between them is less than or equal to a threshold attenuation,  $\beta_{th} = 10 \log(p_r/p_{r,th})$  dB. Now by the log-normal shadow fading model [2], the (on average) probability that a link exists between two VANET nodes, which are at an effective distance  $d_a$  from each other, can be expressed as [1],

$$p_{link} = \frac{1}{2} + \frac{1}{2} \operatorname{erf} \left( \frac{\beta_{th} - \alpha 10 \log(v_a \tau / L)}{\sqrt{2} \sigma} \right) \quad (2)$$

where,  $\alpha$  is the path loss exponent;  $\sigma$  is the standard deviation of a zero mean normal random variable which captures the fading effects. The link probabilities for different values of velocity and a 10 dB perturbation in threshold attenuation are shown in Figure 1 (see [1] for exact parameters.) It can be seen that the link probability is maximum when the vehicles are not moving ( $v_a = 0$ ) which represents congestion on the freeway. As the average velocity starts increasing the probability of a link starts decreasing. Furthermore, it can be observed that a larger value of threshold attenuation allows a higher link probability at all velocities.

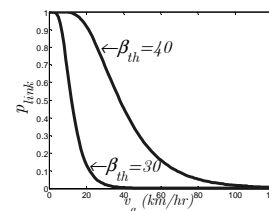


Figure 1. Probability of link between two VANET nodes.

## 3. AVERAGE DEGREE OF VANET NODES

Previous studies have extensively analyzed the connectivity and minimum node degree properties of ad hoc networks (see [5] and the references therein.) We focus on the “average node degree” of the VANET channel. We assume a uniform vehicle density,  $\rho_a$ , throughout this paper. Let the event that a VANET node has a link with  $k$  of the total  $\rho_a - 1$  vehicles in the unit region be denoted by  $\Lambda(k)$ . The (on average) probability of  $\Lambda(k)$  is  $\Pr\{\Lambda(k)\} = \binom{\rho_a - 1}{k} (p_{link})^k (1 - p_{link})^{\rho_a - 1 - k}$ . The average degree of each node then becomes,

$$d_{avg} = (\rho_a - 1) p_{link} \quad (3)$$

where,  $p_{link}$  is given in (2). It is clear that the average degree is directly proportional to the traffic density.

## 4. VANET WORM SPREAD MODEL

Prior studies have successfully modeled the propagation of Internet worms using epidemic models [6], [7]. We employ the *sto-*

chastic SIR epidemic model [3] to capture the spread of active worms over VANET. The *infectious period* of an infected vehicle is exponentially distributed with rate  $\gamma$ , i.e., once infected a vehicle remains in the infected state for a mean time of  $1/\gamma$  after which it transits to the removed state. During its infectious period, an infected node makes contacts with a given vehicle according to a time homogeneous Poisson process with rate  $\lambda$ , i.e., an infected vehicle makes  $\lambda$  contacts with another (given) VANET node in one infectious period. Thus, the time between contacts is exponentially distributed with mean  $1/\lambda$ . If the contacted vehicle is still susceptible then it becomes infected and immediately starts spreading the worm. An infected node after the end of its infectious period becomes removed and plays no further part in the worm spread. The SIR model [3] defines all processes to be independent of each other.

#### 4.1 SIR Model on the VANET Graph

We define a measure, referred to as the *spread factor*, which is the average number of infections (spread by a newly infected vehicle) normalized by the average vehicle density. Mathematically,

$$\text{spread factor} = \frac{E\{\text{infections spread by an infected node}\}}{\rho_a}$$

where,  $E\{\cdot\}$  denotes the expectation operation, and  $\rho_a$  is the average number of vehicles per unit region. Since a susceptible vehicle is infected the first time it is contacted by an infected vehicle, the worm spreading Poisson process can be thought of as the time it takes for an infected vehicle to make the first contact with a given susceptible vehicle. As explained before, the mean time of this *infection process*, which captures the time for the first infectious contact, is exponentially distributed with mean  $1/\lambda$ .

We focus our attention on two worm spread scenarios: (1) *Preemptive Patching*, where a fixed (non-negative) number of nodes,  $\mu \geq 0$ , have been patched before the start of the worm outbreak; (2) *Interactive Patching*, where vehicles are being patched while the worm is spreading. In both cases the probability of infection spread to a node can be written as,

$$\Pr\{\text{infection spread}\} = \Pr\left\{\begin{array}{l} \text{(time for first contact} < \text{infectious period)} \\ \cap \\ \text{(node is unpatched)} \end{array}\right\}$$

We assume that the above two events are independent. Since both the infection process and the infectious period are exponentially distributed,  $\Pr\{\text{time for first contact} < \text{infectious period}\}$  is the probability of *independent competing exponentials*.

#### 4.2 Preemptive Patching

The preemptive patching spread factor can be derived as [1],

$$S_{preempt} = \left(\frac{\rho_a - 1 - \mu}{2\rho_a}\right) \left(\frac{\lambda}{\lambda + \gamma}\right) \left[1 + \text{erf}\left(\frac{\beta_{th} - \alpha 10 \log(v_a \tau / L)}{\sqrt{2}\sigma}\right)\right]$$

Figure 2 illustrates the spread factor for the preemptive patching case (see [1] for exact parameters.) It is evident that, in accordance with the level of preemptive patching, a certain number of nodes are immune to the spread of the worm. The spread factor therefore never reaches one. However, due to the high average

degree in congested scenarios, the worm spreads extremely quickly in the susceptible population. Figure 2 (b) shows that the worm outbreak is somewhat controlled for low-density traffic.

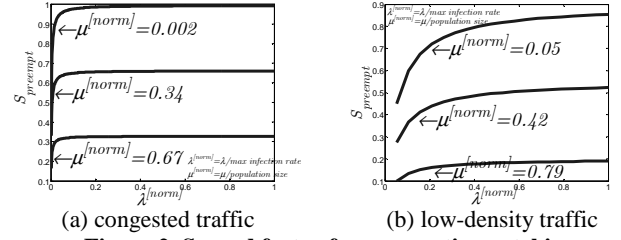


Figure 2. Spread factor for preemptive patching.

#### 4.3 Interactive Patching

We model the *patching process* as a time-homogeneous Poisson process which, for a given infectious period, contacts a vehicle with rate  $\eta$ . The probability that a node is unpatched is then,

$$\Pr\{\text{node is unpatched}\} = \Pr\{\text{time for first infection} < \text{time for first patch}\}$$

Assuming that the patching and infection processes are independent, we can derive the spread factor for interactive patching as [1],

$$S_{interact} = \left(\frac{\rho_a - 1}{2\rho_a}\right) \left(\frac{\lambda}{\lambda + \eta}\right) \left(\frac{\lambda}{\lambda + \gamma}\right) \left[1 + \text{erf}\left(\frac{\beta_{th} - \alpha 10 \log(v_a \tau / L)}{\sqrt{2}\sigma}\right)\right]$$

Figure 3 outlines the interplay between a real-time patching process and the infection process for congested and low-density traffic scenarios (see [1] for exact parameters.) It is clear from Figure 3 (a) that, due to the high average degree of the VANET graph in congested scenarios, the patching rate plays a crucial role in curbing a worm outbreak. While for very low patching rates all susceptible nodes are infected quite rapidly, as the patching rate increases the spread of the worm is mitigated quite effectively. The spread factor for the low-density traffic is even smaller than the congested scenario for all values of  $\eta$ .

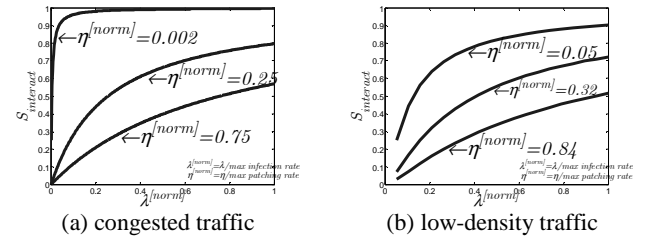


Figure 3. Spread factor for interactive patching.

## 5. REFERENCES

- [1] S. Khayam and H. Radha, "Analyzing the Spread of Active Worms over VANET," Technical Report TR-VANET04, <http://www.egr.msu.edu/waves/publications.htm>.
- [2] T. S. Rappaport, "Wireless Communications: Principles and Practice," Prentice-Hall, 2<sup>nd</sup> ed., 2001.
- [3] H. Andersson and T. Britton, "Stochastic Epidemic Models and Their Statistical Analysis," Springer: Verlag, 2000.
- [4] H. Hartenstein, B. Bochow, A. Ebner, M. Lott, M. Radimirsch, and D. Vollmer, "Position-Aware Ad Hoc Wireless Networks for Inter-Vehicle Communications: the Fleetnet Project," *ACM MobiHoc'01*.
- [5] C. Bettstetter and C. Hartmann, "Connectivity of Wireless Multi-hop Networks in a Shadow Fading Environment," *ACM MSWIM'03*.
- [6] Proceedings of *ACM WORM 2003*.
- [7] Network Security Session, *IEEE Infocom 2003*.