International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, No. 1, April 2010

Worm Spreading and Patching in Inter-vehicle Communications

Lin Cheng and Rahul Shakya

Trinity College, Department of Engineering,
Hartford, CT, USA
{lin.cheng, rahul.shakya}@trincoll.edu

***Abstract*:** Inter-vehicle communications (IVC) rely on frequent data exchange among vehicles to facilitate road safety, congestion control, route planning, etc. The wireless connectivity among vehicles unfortunately poses a challenge for securing large-scale deployment of IVC systems. To successfully mitigate threats such as worm spreading in IVC systems, we describe the potential worm spreading from traffic and propagation modeling. Dual-slope pathloss and shadowing model is used to incorporate propagation and fading effects. Statistical tests performed on traces extracted from real highway data establish the traffic distributions for different times of the day. Potential worm attack and patching are simulated in different traffic scenarios. We also discuss the contributing factors observed.

Keywords: Inter-vehicle communications, worm spreading, patching, traffic**.**

1. Introduction

Over the past decade, the demand for new vehicular communication systems has been growing at a rapid pace. It goes beyond standard passive safety technologies with a number of new active safety applications. Example scenarios include collision warning, hazardous location notifications, congestion control, construction site avoidance, electronic tolls, internet access in vehicles, etc. Initiatives to create new vehicular communication systems have received strong support from academic, government and industry in recent years. Inter-vehicle communication (IVC) is one of the key enabling technology for these applications [1]. As part of the intelligent transportation systems for dedicated short range communications [2], frequency band around 5.9 GHz is allocated in different parts of the world (for example, 5.85 to 5.925 GHz in USA) [3].

The wireless connectivity among vehicles unfortunately poses a challenge for securing large-scale deployment of IVC systems. Consider the increasing use of onboard computers on vehicles, the likelihood of worm infection keeps increasing. Owing to the broadcasting nature of IVC emergency messages, worm infection or other security alerts may propagate as well, creating more security threats along the highway.

Reported works on worm spreading include modeling the worm epidemics in high-speed networks [5]. The authors in [6] analyzed the requirements on worm mitigation techniques in Mobile Ad Hoc Networks. [7] presented the modeling on worm epidemics in vehicular ad hoc networks, while [8] is dedicated to model the spread of active worms. The authors in [9] discussed the the spread of active worms over IVC systems.

To successfully mitigate worm spreading in IVC systems, it is important to understand what is special on IVC communications and the nature of IVC message propagation.

- In an IVC system, both the transmitter and receiver are moving with high speed. IVC connections may be highly dynamic and may have reduced duration of communication links.
- These communication links may experience pathloss and shadow-fading owing to the objects on the road and around the environment as vehicles transverse diverse environments.
- IVC systems may be employed in different traffic scenarios (light/dense traffic) and/or market penetrations. This will have an impact on the message as well as the worm propagation.

Taking into account the above features, Inter-vehicle communication systems that can successfully mitigate worm spreading are in need for physically meaningful models to mimic message propagation.

2. Traffic and Mobility Modeling

Before we describe any mitigation strategy for IVC, it is critical to understand the key features of IVC traffic and mobility features. It is important to note the difference between IVC and mobile ad hoc network (MANET) systems. On the mobility side, results from MANETs such as random walk cannot be applied, as IVC systems' movement are more constrained by the road network.

Traffic models in IVC systems refer to the mathematical characterization of flows generated by various on-road vehicles. With network performance being highly dependent on the actual traffic, it is obvious that accurate traffic models are needed. One of the widely used methods to describe traffic behavior is the car following model from civil engineering. The authors in [10] have extended the car-following model to the road-level

$$S = L_{min} + \beta V. \qquad (1)$$

where S is the headway spacing between rear bumper to rear bumper, V is the vehicle speed in meters/second, β is the inter-arrival time of vehicles on any lane of the same road as observed from a fixed observation point, and L_{min} is the minimum spacing between any two adjacent vehicles.

Instead of counting on (may be unrealistic) assumptions, our approach to traffic modeling is "data driven." We model the traffic empirically from the real-life highway data collected by dual-loop detectors from Berkeley High-way Laboratory [11]. The measurements were conducted in a 24 consecutive hour period on a multi-lane highway I-80 in California.

50289 cars were reported in the measurements in this 24 hour period, the resolution of the time stamp is 0.01666 second. With different times of the day, this represents different scenes in real-life traffic.

We monitored the arrival processes at different times of the day and modeled their corresponding traces. These empirical traces were further modeled using Kolmogorov-Smirnov test (K-S test) to evaluate the fit to the empirical distribution. We used the K-S test because this test statistic does not depend on the underlying cu-mulative distribution function being tested. In addition, as opposed to tests that depend on an adequate sample size to obtain valid approximations (e.g., the chi-square goodness-of-fit), the K-S test is a rigorous test that does not have dependency on binning. The biggest discrepancy find between samples from the empirical distribution and candidate analytical distribution is referred to as the D-statistic. The best-fit result is the one who exhibits the smallest D-statistic.

We pick representative 2-hour periods to describe here. 15-17 represents busy hours in the afternoon, they stay in the left-upper corner since TR separation is tighter than other times. 10am-12pm is a representative case of moderate traffic conditions. Finally, 1-3am is the least crowded time of the day.

The result of the K-S test for these three 2 hour period is summarized in Table 1. Extreme light traffic is best described by exponential (EXP) distributions, while the other two periods follow Generalized extreme value (GEV) distributions. An exponential distribution has only one parameter μ, while a Generalized extreme value (GEV) distribution has three (K, σ and μ).

Time	Type	Parameters of the best fit distribution			
		K	σ	μ	D-statistic
1-3	EXP	N/A	N/A	259.28	0.027
10-12	GEV	0.29	17.12	20.43	0.023
15-17	GEV	0.02	0.20	8.87	0.039

Table I. CAR SEPARATION DISTRIBUTIONS

Very similar to the above method, we modeled the vehicle velocity from real traffic too (omitted owing to space limitations). The traffic traces to be generated for worm spreading and patching is now under control and mimic the real on-road data, thus, we can effectively achieve a wide range of simulation experiments using the traffic model. In what follows, we apply it to our worm spreading/patching applications.

The above features describe the particular traffic context of communication in IVC, these characterizations will be integrated into the worm mitigation modeling taking into account these features.

3. Simulating Worm Spreading and Patching

For worm spreading and patching simulations a 10 km long highway corridor was generated by sampling the car separation distribution during different times of the day.

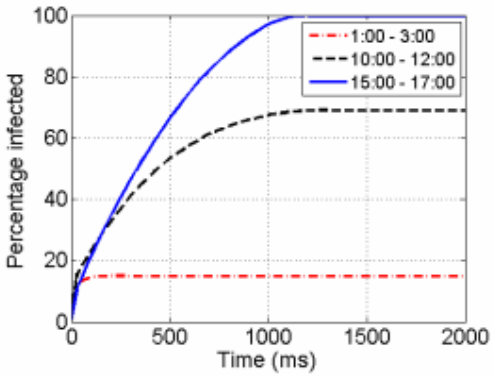
The IVC shadow-fading propagation model was derived from our earlier work on IVC channel sounding measurements [12]. We found that a dual-slope piecewise-linear model is able to represent the measurements more accurately. We characterize this piecewise model by a path loss exponent and standard deviation representing shadowing effects.

For a given time of the day (which also represents different traffic patterns), the transmitter-receiver (TR) separation and velocities were generated to mimic real traffic. Propagation model is then applied based on this TR separation. It is worth noting that we have assumed a frozen traffic network (will remove this constraint in future work).

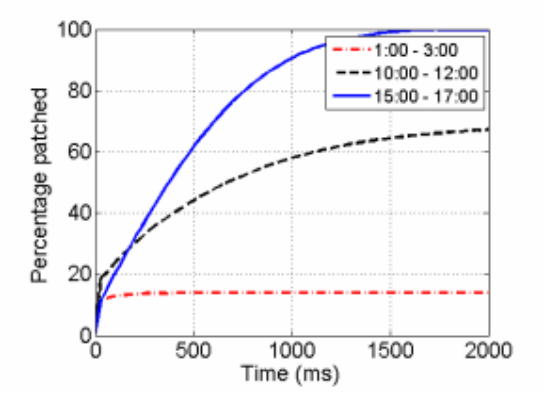
For worm spreading, a randomly selected vehicle was infected and was allowed to broadcast it messages. Here any neighbor vehicle within the broadcast range would automatically get infected and would rebroadcast the malicious message. For our simulation purposes we have used the timeout between rebroadcasts to be 30ms, although it is set to a parameter that can be changed easily.

We then consider the following scenario: while the worm is spreading in the vehicular network, vehicles can also get patched against the worm in real-time. For example, vehicles could download patches from roadside units using vehicle-to-roadside communications. The vehicle who successfully got patched first can forward this patch to other vehicles in the network, using one or multiple hops. The spread of the patching could also occur in a mechanism similar to the worm spreading. In our simulations, rebroadcast would follow a protocol where contention windows are assigned to neighbors according to the distance from the transmitting node. To be precise, let L be the maximum range of a single hop. According to certain bin size, we divide the distance L into multiple zones. A contention window of duration τ is associated with each zone. If vehicle 1 transmits the patching message along with its GPS coordinates, the rest of vehicles in the vicinity will determine which zone they belong to based on the GPS coordinates, relative to vehicle 1. Each vehicle node will wait for its contention window, with the furthest contention bin allowed to transmit first. Here, if a node in a lower contention bin hears a rebroadcast it will cancel its own rebroadcast. For this set of simulations, we have used six contention bins, each bin is 50 meters long (although it is set to a parameter that can be changed easily).

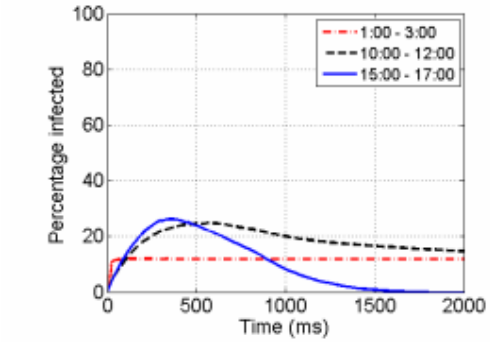
The above protocols were used in simulations for worm spreading, patch spreading and the scenario when they occur simultaneously. For each scenario, results were averaged for 100 simulation runs.



(a) Worm spreading at different times of the day.



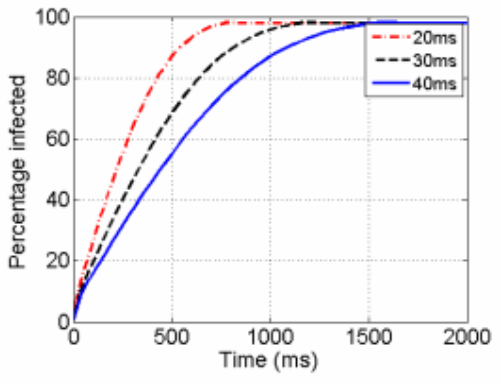
(b) Patching at different times of the day.



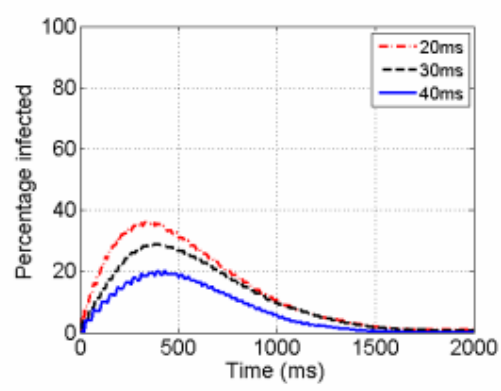
(c) Worm and patch spreading at different times of the day.

Figure 1. Simulated results for realistic traffic scenarios.

In the first set of experiments, the timeout between rebroadcasts is set to 30 ms. Fig. 1(a) depicts the percentage of vehicles got infected during worm spreading in traffic for different time of the day, while Fig. 1 (b) describes the percentage of vehicles got patched vs. time, as vehicle with the patch propagate this data to others. These results indicate that worm spreading and patching occur at different speeds and have different penetration depending on the time of the day. During peak afternoon rush hours (The vehicle density is approximately 85 vehicles per kilometer), any worm or patch that has entered the scenario could ultimately affect the entire highway. During morning rush hours (The vehicle density is about 30 vehicles per kilometer), approximately 70% of car are affected. In the early AM hours (The vehicle density is approximately 5 vehicles per kilometer), only 15% of the cars were affected. Results from sparse traffic reflect the fact that due to low vehicle density, nodes are disconnected from each other. Similarly, we observe that patching rate is relatively slower than worm spread rate, which can be attributed to the usage of contention windows. When worm spreading and patching occur simultaneously (Fig. 1(c)), we observe that though the number of infected vehicles initially increases, it gradually falls off when the worms are finally under control by patches. For afternoon and morning rush hours we find that at the peak value, a maximum of 26% of the cars are infected, where after infected vehicles begin to get patched. For the early AM hours, the fact that some vehicles still remain infected indicates that the vehicles are disconnected from each other and thus some infected vehicles are unable to receive patches.



(a) Worm spreading at different timeout between rebroadcast.



(b) Worm spreading and patching at different timeout between rebroadcast.

Figure 2. Experiments with different timeout between rebroadcast.

In the second set of experiments, we vary the timeout between rebroadcast of the worm, we find that propagation speed is scaled likewise (Fig. 2(a)). We observe that varying worm rebroadcast timeout (20ms, 30ms, and 40ms) (while keeping patch rebroadcast speed constant (at 30ms)) has a noticeable effect upon the infection spread rate and maximum penetration (Fig. 2(b)). When worm rebroadcast speed is lower than that of the patching, up to 36% of vehicles are infected, while when worm rebroadcast speed is greater than that of the patch, only up to 20% of vehicles are infected.

4. Conclusion

Information exchange among vehicles poses a great challenge for securing large-scale deployment of IVC systems. It is important to have effective mitigate strategies to deal with threats such as worm spreading in IVC systems in different traffic and propagation scenarios. We describe the potential worm spreading and patching, using traffic and propagation modeling. Worm spreading and patching

behaviors are simulated and observations were made for the correlation to different traffic scenarios.

References

[1] W. Chen and S. Cai, "Ad hoc peer-to-peer network architecture for vehicle safety communications," IEEE Commun. Mag., vol. 43, no. 4, pp. 100–107, Apr. 2005.

[2] T. Kosch and W. Franz "Technical concept and prerequisites of car-to-car communication," Proc. 5th Eur. Congr. Exhib. Intell. Transp. Syst. Serv., Hannover, Germany, Jun. 2005. pp. 1–12.

[3] IEEE P802.11p/D2.01, "Standard for wireless local area networks providing wireless communications while in vehicular environment," Tech. Rep., Mar. 2007.

[4] J. Hubaux, S. Capkun, and J. Luo, "Security aspects of inter-vehicle communications," IEEE Security & Privacy Magazine, vol. 2, pp. 49–55, 2005.

[5] T. Chen and J-M Robert, "Worm epidemics in high-speed networks," IEEE Computer, pp. 48–53, 2004.

[6] R. Cole, N. Phamdo, M. Rajab and A. Terzis, "Requirements on worm mitigation techniques in MANETs," Proc. of the Workshop on Principles of Advanced and Distributed Systems.

[7] M. Nekovee, "Modeling the spread of worm epidemics in vehicular ad hoc networks," IEEE Vehicular Technology Conference, 2006.

[8] Z. Chen, L. Gao, and K. Kwiat, "Modeling the spread of active worms," IEEE INFOCOM, 2003.

[9] S. Khayam and H. Radha, "Analyzing the spread of active worms over vanet," Proceedinsg of VANET, 2004.

[10] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in sparse vehicular ad hoc wireless networks," IEEE Journal on Selected Areas in Communications, vol. 25, 2007.

[11] University of California, Berkeley Highway Laboratory (BHL), http://sprocket.ccit.berkeley.edu/bhl

[12] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrowband channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band," IEEE J. on Select. Areas in Commun., vol. 25, no. 8, pp. 1501–1516, Oct. 2007.