Worm Epidemics in Vehicular Networks

Oscar Trullols-Cruces, *Student Member, IEEE,* Marco Fiore, *Member, IEEE,*
Jose M. Barcelo-Ordinas, *Member, IEEE*

Abstract—Connected vehicles promise to enable a wide range of new automotive services that will improve road safety, ease traffic management, and make the overall travel experience more enjoyable. However, they also open significant new surfaces for attacks on the electronics that control most of modern vehicle operations. In particular, the emergence of vehicle-to-vehicle (V2V) communication risks to lay fertile ground for self-propagating mobile malware that targets automobile environments. In this work, we perform a first study on the the dynamics of vehicular malware epidemics in a large-scale road network, and unveil how a reasonably fast worm can easily infect thousands of vehicles in minutes. We determine how such dynamics are affected by a number of parameters, including the diffusion of the vulnerability, the penetration ratio and range of the V2V communication technology, or the worm self-propagation mechanism. We also propose a simple yet very effective numerical model of the worm spreading process, and prove it to be able to mimic the results of computationally expensive network simulations. Finally, we leverage the model to characterize the dangerousness of the geographical location where the worm is first injected, as well as for efficient containment of the epidemics through the cellular network.

Index Terms—Vehicular networks, V2V, mobile malware.

1 Introduction

Pervasive wireless device-to-device (D2D) communication is regarded as a game changer that could enable a broad range of new applications in a wide range of contexts. However, if not properly secured, the network interfaces of smart devices can turn into easily exploitable back-doors, allowing illegal remote access to the information stored on the device as well as to the local network it may be connected to. Even worse, D2D communication can be leveraged by self-propagating malware to reach a large number of devices and damage them, disrupt their services or steal sensible data.

Although mobile malware first appeared a decade ago [2], [3], [4], the low penetration of smart devices and the heterogeneity of their operating systems have prevented major outbreaks to date [5]. Yet, as the diffusion of communication interfaces keeps growing and the OS market becomes more stable, we may face smart-device worm epidemics in the near future. In fact, the research community has started assessing the risks associated to a large-scale diffusion of so-called *mobile worms*. Simulative and experimental studies have considered epidemics in campuses [6] or urban areas [7], and different infection vectors, from metropolitan Wi-Fi associations [8] to text messaging in cellular networks [9], [10].

A quite underrated context where mobile malware could cause dramatic damage is the automotive one. Indeed, vehicles feature today a wide range of Electronic Control Units (ECUs) that drive most of the car automatic behaviors and are interconnected by a Controller Area Network (CAN) bus. Experimental tests have demonstrated that ECUs are extremely fragile to the injection of non-compliant random messages over the CAN. Even worse, a knowledgeable adversary can exploit them to bypass the driver input and take control over key automotive functions, e.g., disabling brakes or stopping the car engine [11]. Remote attacks on ECUs have been proved feasible via the Tire Pressure Monitoring Systems (TPMS) [12] or the CD player, Bluetooth and cellular interfaces [13].

In a context where awareness of the security risks associated to connected vehicles is growing [14], [15], D2D technologies for vehicular environments, enabling direct vehicle-to-vehicle (V2V) communication, are nearly upon us. Regulators in the US are already crafting a proposal enforcing all new vehicles to embed V2V radio interfaces by early 2017 [16]. Despite the advantages it will bring in terms of support to road safety and traffic management services, the emergence of the V2V paradigm risks to significantly widen the range of attack surfaces available to vehicle-targeted mobile malware [17]. Understanding the dangers associated with a vehicular malware epidemics becomes then critical.

In this paper, we contribute to that endeavor by providing a first comprehensive characterization of the dynamics of a mobile worm that exploits V2V communication to self-propagate through a large-scale road network. To that end, after a review of the literature, in Sec. 2, we first identify the major properties of a generic vehicular worm, in Sec. 3, and present our reference road traffic scenarios, in Sec. 4. In Sec. 5, we propose a data-driven numerical model of the worm propagation process that is at a time simple and accurate. We then unveil, in Sec. 6, the significant features of a vehicular worm epidemics in a very large-scale environment. Sec. 7 provides an in-depth analysis of the dangerousness of worms injected at different geographical locations, and proposes a practical technique for the containment of worm epidemics, which achieve a 100% healing of infected nodes while reducing patch transmissions by up to 90% with respect to a naive approach. Finally, Sec. 8 concludes the paper.

2 Related Work

Despite the significant danger represented by the appearance of mobile malware in vehicular environments, the literature on the topic is still relatively thin. Indeed, surveys on automotive security only recently started to acknowledge V2V-based

This work is an extended version of a IEEE WoWMoM 2013 paper [1].

O. Trullols-Cruces and J. M. Barcelo-Ordinas are with UPC, 08034 Barcelona, Spain. M. Fiore is with CNR-IEIIT, 10129 Torino, Italy.

The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Unions Seventh Framework Programme (FP7/2007-2013) under REA grant agreement n.630211, and has been supported by Spanish National project TIN2013-47272-C2-2-R.

malware as a major threat [18], [19].

In a seminal work, Khayam and Radha [20] perform a first analytical study of vehicular worm spreading on a highway. In order to make the model tractable, their analysis relies on average values rather than on a complete description of the network connectivity. Nekovee [21] remarks that such an approach fails to capture the spatiotemporal dynamics of V2V connectivity and overestimates the rapidity of the infection. In order to account for the time-evolving nature of the vehicular network, Nekovee uses a set of snapshots of the road traffic, and simulates the diffusion of a worm in each separately. Although he employs realistic microscopic mobility models to derive road traffic densities, Nekovee assumes uniform distributions of vehicles, which have later been shown not to occur in the real world [22], [23].

Chen and Shakya [22] overcome the problem by populating highway traffic snapshots according to inter-vehicle spacing distributions fitted on real-world data collected by researchers of the Berkeley Highway Laboratory. The availability of such dual-loop detector data for different daily traffic conditions allows to explore the impact of daytime on the worm epidemics. However, the lack of temporal correlation between the snapshots does not allow to study the propagation of worms over time; this, in turn, precludes the possibility of leveraging the model in systems where car positions change during the spreading process, e.g., in presence of roads longer than a few kilometers or of worms that take more than a few milliseconds to self-propagate. For the same reason, this technique cannot capture diffusion through store-carry-and-forward, where vehicles physically transport the malware until the latter can infect other cars during occasional contacts.

Wang *et al.* [24] properly account for such temporal features by leveraging tools for the simulation of both road traffic and vehicular network operations. The approach allows to evaluate how worm epidemics are affected by several system parameters, i.e., the communication range, the density of vehicles, and the medium access control mechanism. The study by Wang *et al.* represents, to the best of our knowledge, the only other work on an urban scenario: however, their road network is modeled as a simple Voronoi tessellation, and it covers a small surface of 1 km^2 with less than 200 vehicles.

When compared to the previous works above, our study yields the following original contributions:

- Our evaluation is carried out on a scale that is orders of magnitude larger than those considered in the literature: considering a 10.000 km^2 region with over 3.600 km of heterogeneous roads allows us to picture vehicular worm epidemics with unprecedented breadth an detail;
- Our analysis is performed on different state-of-art datasets of road traffic that yield realistic macroscopic and microscopic features: we do not thus rely on simplistic assumptions on the features of vehicular mobility – an approach that substantiates the reliability of our results;
- We propose an original numerical model of vehicular worm propagation, which leverages statistical road traffic data commonly available to transportation authorities; the model is simple, yet it can accurately reproduce the epidemics in realistic mobility conditions and for the whole space of system parameters, capturing worm diffusion via both connected multi-hop and store-carry-and-forward paradigms.

The spreading of generic vehicular worms can also be assimilated, to some extent, to the dissemination of information in vehicular networks. Research activities in that context have mainly focused on: (i) simulative analyses of the dissemination of delay-tolerant data within urban areas; (ii) analytical modeling of epidemic dissemination in highway environments.

As far as the first category is concerned, efficient protocols such as MDDV [25] and VADD [26], just to cite a couple of well-known approaches, are built around complex decision algorithms that minimize the communication overhead while preserving high packet delivery ratios and low delays. These works are thus different in spirit from ours, where worms propagate in a completely uncontrolled fashion, and without any concern on the overhead they generate. Such epidemic dissemination in urban vehicular networks has been also studied [27], although in scenarios spanning a few tens of km^2, and without proposing an actual modeling of the phenomenon.

Also when confronted to the second type of works, all of our major contributions listed above still hold. In addition, epidemic dissemination models typically build on strong assumptions on, e.g., deterministic [28] and exponential [29], [30] inter-vehicle spacing distributions, or on independently distributed speeds of vehicles [31], [32]. As already discussed, our study is instead based on realistic road traffic datasets. Finally, as we deal with malware rather than normal content, we address aspects – such as the worm containment or the level of danger associated to geographical locations – that are not considered in epidemic dissemination.

3 Mobile worms in vehicular networks

Worms are programs that self-propagate across a communication network through security flaws common to large groups of network nodes; they are thus different from computer viruses in that the latter need the intervention of the user to propagate. Worms can be classified on the basis of several factors [33]: the *target discovery*, i.e., the way they discover targets to propagate to; the *carrier*, i.e., the infection mechanism used for the self-propagation; the *activation*, i.e., the technique by which the worm code starts its activity on the infected host; the *payload*, i.e., the set of routines undertaken by the worm, that clearly depend on the nature and objective of the attacker.

Our interest is on the worm epidemics within the vehicular network. Therefore, in this paper we focus on the first two aspects above, the type of target discovery and the kind of carrier employed by the worm, as they mainly drive the malware self-propagation process. Our study is instead activation- and payload-independent, since we do not delve into the kind of damage caused by the worm nor the motivation behind the attacks – although the discussion in Sec. 1 hints at how dangerous the outcome could be.

In the remainder of this section, we will characterize vehicular worms in terms of their target discovery and carrier features. We will also introduce the overall worm infection process which we will assume in our study.

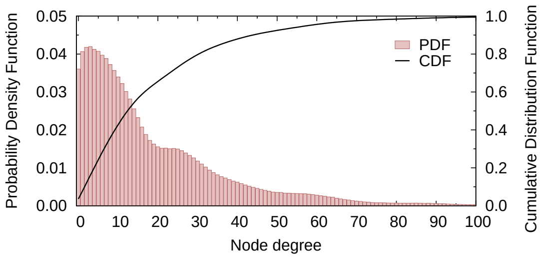


Fig. 1. Distribution of the node degree in the vehicular network of the Canton of Zurich dataset.

3.1 Target discovery

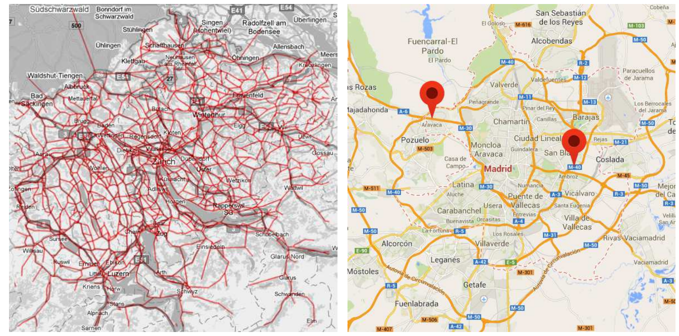
The target discovery of a worm within a vehicular network is dictated by the dynamics of road traffic. As a matter of fact, the relatively short range of V2V communication limits the set of potential worm targets to cars in geographic proximity of the one the worm resides in. Thus, it is the physical mobility of cars that allows the worm to enlarge its target set, by exploiting links established between communication-enabled vehicles that come into contact during their trips.

Such a *mobility-driven geographic target discovery* occurs in a way that significantly differs from that of standard Internet worms, which have to perform global or local scans for IP addresses to infect. In vehicular networks, the target discovery is implicitly (and involuntarily) supported by the forthcoming V2V communication standards, that mandate the periodic broadcast of beacon messages by all vehicles and with high (1 to 10 Hz typically) frequency: this is the case of, e.g., SAE J2735 heartbeats (part of the WAVE stack) and ETSI ITS Cooperative Awareness Messages (CAMs). A worm could then simply leverage the information collected by the vehicle via these messages in order to determine its current target set.

3.2 Carrier

As far as the carrier is concerned, two mechanisms are possible. In the first case, the worm can self-propagate through broadcast messages, infecting all of its neighbors at once. We refer to this mechanism as the *broadcast carrier*. In the second case, the worm can only propagate to one neighboring vehicle at a time, which we tag as *unicast carrier*. We argue that, in the case of a unicast carrier, no real decision has to be taken on which communication neighbor to attack: unlike what happens in the Internet, where the choice is between hundreds of millions of machines, the number of cars concurrently in range of a worm is generally low. As an example, in the large-scale road traffic scenario we will detail in the next section and consider in our analysis, the distribution of the number of one-hop neighbors (i.e., the vehicular network node degree) follows Fig. 1. The degree ranges from a few units to a few tens of vehicles at most, and a car typically has less than 10 neighbors half of time. Such a small target set size makes a selection of the target node subset pointless, and worms can randomly pick the neighbor car to infect next.

The carrier is also characterized by a second aspect, i.e., the number of transmissions (either broadcast or unicast) required to complete the infection. This value depends on the size of the worm (in KB) and on the way it is hidden into messages.



(a) Canton of Zurich, road map (b) Madrid, highway segment locations

Fig. 2. (a) Road network layout in the Canton of Zurich dataset, scaled at 1:2.700.000. (b) Geographical location of the highway segments in the Madrid dataset.

We translate this aspect into a second parameter, the *carrier latency* τ, i.e., the amount of time a worm needs to self-propagate to all (broadcast carrier case) or one (unicast carrier case) of its neighbors. Thus, τ also accounts for all delays possibly incurred in at different layers of the stack: e.g., association and session establishment procedures, wireless channel contention or lost message retransmissions.

3.3 Worm infection process

Borrowing the terminology from epidemiology, we adopt in our study a Susceptible, Infected, Recovered (SIR) model with Immunization. According to this model, a clean node is *susceptible* to become *infected* by the worm, but it is *healed* if it receives a dedicated cure, i.e., a patch, that prevents it from contracting the infection again. The same cure can be delivered even to a susceptible node, which is then *immunized*, i.e., it cannot be infected by the worm[1]. We also denote the first infected vehicle as *patient zero*, and the location and time at which it was first infected as the *origin* of the worm infection.

The population affected by the SIR model with Immunization is formed by all communication-enabled vehicles that circulate in the geographical area of interest, and suffer from the security flaw exploited by the worm to propagate. We characterize such a fraction of vehicles through the *penetration ratio* ρ, which thus accounts for the diffusion of both the vehicular communication technology and the security flaw.

4 Reference scenarios

We employ two types of road traffic datasets in our study. The first is a large-scale representation of vehicular mobility within the *Canton of Zurich*, in Switzerland. We employ this dataset as our reference scenario for the investigation of malware epidemics over a wide geographical region. The second is a set of accurate descriptions of highway traffic along two segments of the beltway surrounding *Madrid*, Spain. We leverage this

1. We favor a SIR model over other common models, such as Susceptible-Infected-Susceptible (SIS), as we believe that it better fits the threat use case we consider. Indeed, we assume the mobile worm to self-propagate among connected vehicles without human intervention. The worm thus exploits some backdoor or software vulnerability to infect a new vehicle, rather than thoughtless actions by a human actor. Hence, a patch that solves the software flaw can prevent further infections by the same mobile worm.

latter dataset for the fine-grained calibration and validation of our numerical model of the vehicular worm propagation.

Both datasets are synthetic, yet they faithfully mimic the features of real-world road traffic. Below, we present the two datasets, and motivate their choice for the purpose of our study.

4.1 Canton of Zurich dataset

Our reference scenario encompasses the whole Canton of Zurich, an area of 10.000 km^2 in Switzerland. The region, whose 3.683-km road layout is portrayed in Fig. 2(a), comprises the urban and suburban neighborhoods of Zurich, several smaller towns nearby, as well as the highways, freeways and minor regional roadways interconnecting them. The synthetic mobility of vehicles in the area has been generated by means of the multi-agent microscopic traffic simulator (MMTS) developed at ETH Zurich. The MMTS queuing-based mesoscopic modeling approach has been proven to reproduce real-world large-scale traffic flow dynamics and small-scale car-to-car interactions [34].

The choice of this dataset for our large-scale study of vehicular worm epidemics is an unescapable one. Indeed, no other synthetic or real-world mobility dataset that is publicly available covers today a similarly wide region in a comparable realistic manner. Other synthetic datasets may feature higher microscopic detail [35], [36], however they cover geographical areas that are two orders of magnitude smaller than that included in the Canton of Zurich dataset. Even real-world data on vehicular mobility, logged from taxis [37], [38] or buses [39], cannot compete in terms of spatial coverage; moreover, such data is only representative of a limited subset of road traffic. Overall, using alternate datasets would significantly limit the scope and interest of our analysis.

4.2 Madrid dataset

The Madrid dataset comprises 16 traces of road traffic on two highway segments in proximity of Madrid, Spain. The geographical locations of the two highways are portrayed in Fig. 2(b): the left marker pinpoints a segment of the A6 motorway that connects A Coruña to Madrid, the right one identifies a segment of the M40 that runs around the conurbation. The traces represent vehicular mobility on each highway segment at rush (8 am) and off-peak (11 am) hours on four working days. The traces were generated by feeding fine-grained real-world traffic counts to a microscopic simulator implementing well-known car-following and lane-changing models. They feature free-flow traffic in quasi-stationary conditions [40].

The Madrid dataset is the most realistic description of road traffic on individual highway segments that is publicly available to date. It thus represents the sensible choice for the calibration and validation of our numerical model of the worm propagation speed along single road segments, in Sec. 5.2.

5 MODELING THE WORM EPIDEMICS

The computer simulation of worm epidemics in the large-scale scenario presented in Sec. 4.1 is computationally expensive. The span of the road topology – where up to 36.000 vehicles travel concurrently for a time span of several hours – prevents the use of traditional network simulators, such as ns-3 or OMNeT++. Instead, we developed a dedicated simulator[2] that abstracts the detailed processing of messages through the network protocol stack, and adopts a simple R-radius disc modeling of the radio-frequency signal propagation. Unless stated otherwise, we will consider a default V2V communication range R = 100 m. This represents an average value among those identified for reliable packet delivery by different experimental studies on DSRC-based transfers [41], [42].

Such a design makes simulations of very large-scale vehicular networks more bearable. In Sec. 6, we will leverage simulations to provide first qualitative insights into the epidemics dynamics, in presence of different carrier types, penetration ratios, V2V communication ranges and infection origins.

However, even such a scalable simulation approach remains limited by its computational cost, which does not allow to perform comprehensive, quantitative analyses. To overcome this issue, we propose a numerical model capable of faithfully mimicking the vehicular worm epidemics. Our broadcast-carrier worm propagation model is data-driven, in that it is based on commonly available road traffic statistics. Although simple in its expression, the model can capture the impact of a number of system parameters on the large-scale worm propagation delay, at a computational cost that is orders of magnitude lower than that of a simulative evaluation. We devote this section to the description and validation of the model, which we will later exploit in Sec. 7 to carry out extensive studies that are not feasible via simulation.

5.1 Preliminaries

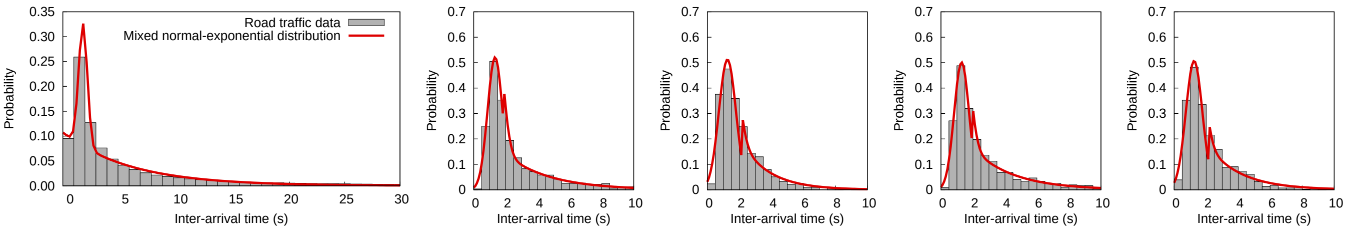
Most existing analytical models of information propagation along road segments build on strong assumptions on the nature of vehicle inter-arrivals, so as to make the problem mathematically tractable. As discussed in Sec. 2, many such models presume, e.g., deterministic or Poisson arrivals. However, measurements on real-world arterial roads have shown that actual vehicular inter-arrival times follow a more complex normal-exponential mixture distribution [23], i.e.,

$$f_T(t) = w_N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(t-\mu)^2}{2\sigma^2}} + w_E \lambda e^{-\lambda(t-t_0)}, \qquad (1)$$

where μ, σ, λ and t_0 are the parameters of the normal and exponential components, respectively, whereas w_N and w_E are their associated weights. Clearly, the discrepancy between the assumed and actual arrival distributions questions the validity of many models proposed in the literature.

Instead, our model does not require any assumption on the distribution of vehicle inter-spacing, speed or inter-arrival time. As we will later detail, the model operates on averages only, which makes it independent of higher order statistics and capable of accommodating any distribution. This notwithstanding, we make sure that our model is evaluated under inter-arrival settings that faithfully mimic those encountered in the real world. Specifically, we verified that the reference

2. URL: `http://people.ac.upc.edu/trullols/downloads.html`.



(a) Zurich (b) A6, May 10, 8 am (c) M40, May 10, 8 am (d) A6, May 11, 8 am (e) M40, May 12, 11 am

Fig. 3. Inter-arrival time distributions. (a) Canton of Zurich. (b,c,d,e) Madrid highways at different days and hours.

scenarios used in our study and introduced in Sec. 4 yield inter-arrival distributions that match the normal-exponential mixture identified by empirical measurements. Fig. 3 portrays the inter-arrival distributions observed in the Canton of Zurich dataset and in four Madrid traces: in all cases, the synthetic road traffic data follow the mixture theoretical distribution in (1).

The numerical model we propose builds on (i) information about the road topology and (ii) statistical information about the road traffic. In the first category, we need, for each road segment[3] i, knowledge of its length l_i and a list of the other roads it intersects with: this data can be easily extracted from accurate road mapping services such as, e.g., OpenStreetMap. As for the second category, the model requires information on the average travel speed $v_i(t)$ on road segment i at time t, and on the mean inter-arrival time $a_i(t)$ of vehicles at road segment i at time t. Such road traffic metrics are typically collected by transportation authorities and automobile service providers through induction loops, infra-red counters, traffic monitoring cameras, and, more recently, floating car data [43]. Therefore, historical or statistical data on measures such as $v_i(t)$ and $a_i(t)$ is available for large portions of the road topology, and its public disclosure is growing, fostered by open data initiatives.

As road traffic information is, by its own nature, time-varying, the average speed and inter-arrival time are not the same over the day or on different days of the week, which is why we consider $v_i(t)$ and $a_i(t)$ to be dependent on time. The aforementioned historical or statistical data already reflects this aspect, with finite yet representative time granularity[4]. We also remark that, although higher order statistics may be available to transportation authorities or automobile service providers, our model only requires knowledge of the mean values of $v_i(t)$ and $a_i(t)$ during each time period. This keeps the model simple and computationally efficient, at the same time avoiding to raise privacy or security issues related to the disclosure of exceedingly detailed data about road traffic dynamics.

In the remainder of this section, we will discuss how the aforementioned information is leveraged to build our model, following the notation summarized in Tab. 1. Specifically, in Sec. 5.2, we will present a model of the worm propagation speed along a single road segment. Then, in Sec. 5.3 we will extend the result to a network-wide infection process.

3. The model can accommodate any definition of *road segment*, and can adapt to the detail level of available road traffic statistics. In our study, we map road segments to (i) segments between any two intersections in the Canton of Zurich scenario, and (ii) 10-km highway stretches in the Madrid dataset.

4. In our evaluation, we assume that statistical data on the road traffic is aggregated and updated with a time granularity of 15 minutes, largely sufficient to capture the temporal variability of road traffic.

TABLE 1
Summary of notation.

τ	Carrier latency – amount of time a worm needs to self-propagate
ρ	Penetration ratio – fraction of communicating vehicles susceptible of infection
R	Communication range – maximum distance for two vehicles to communicate
v_i	Average traval speed on road i
a_i	Average inter-arrival time on road i

5.2 Per-road segment worm propagation

Our goal is initially to model the *worm propagation speed* $s_i(t)$ along a segment i at time t, characterized by average road traffic parameters $v_i(t)$ and $a_i(t)$, while accounting for R, ρ and τ. For the sake of clarity, in the following we will refer to a generic time instant and drop the time notation.

We start from the consideration that the worm propagation speed mainly depends on the network connectivity level. Namely, the malware can propagate wirelessly, and thus at a high speed, in a well-connected vehicular network where multi-hop communication can take place. Conversely, the worm propagation is slowed down when communication opportunities are scarce. Focusing on the two extreme cases, we can state that: (i) in complete absence of vehicle-to-vehicle connectivity, the worm propagates at the vehicular speed v_i, as it is physically carried by isolated cars; (ii) in presence of a complete road coverage by a very dense multi-hop vehicular network, the worm proceeds by jumps of distance equal to the communication range R, each needing a time τ (i.e., the carrier latency) to complete, during which the worm still moves at speed v_i. Thus, the worm propagation speed can be written as

$$s_i = v_i + \frac{R}{\tau} f(a_i, v_i, \rho, R, \tau) \;, \tag{2}$$

where $f(\cdot)$ is a function that describes how the vehicular network connectivity depends on the different system parameters. The function returns values between 0 (complete absence of connectivity, all vehicles are isolated) and 1 (fully connected network, any pair of cars is connected via a multi-hop path).

In order to characterize the exact expression of $f(\cdot)$, we consider the impact of the different parameters on the network connectivity. Let us start from the simplified case of vehicles moving along the same road direction. In that case, the average distance between two subsequent vehicles is given by $a_i \cdot v_i$, i.e., the distance traveled by the first vehicle before the following one enters the same road. The penetration ratio can be accounted for by assuming that the first vehicle is equipped with a V2V radio interface and vulnerable to the worm, and ρ can be seen as the probability that the following vehicle

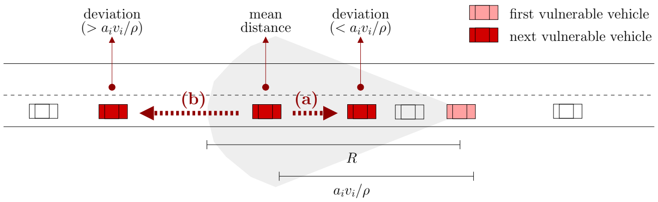


Fig. 4. Example of the negative impact on network connectivity of the deviation of an individual vehicle speed and inter-arrival time from the mean values v_i and a_i.

is communication-enabled and vulnerable as well. Then, an average of $1/\rho$ vehicles must enter the road before a second car susceptible of being infected appears on the same road. The average distance between to vehicles that can be involved in the epidemics is then $\frac{a_i v_i}{\rho}$.

The connectivity is determined by the relationship between the distance above and the transmission range R. In particular, it is the ratio between the two values, $\frac{a_i v_i}{\rho R}$, that matters: the lower the ratio, the higher the network connectivity, and vice-versa. In fact, it is to be noted that those above are all average values, and that some variability is natural in both the inter-arrival time and speed of individual vehicles. As shown in Fig. 4, the actual distance between vulnerable vehicles can be lower (case (a), next vehicle shifted towards the first) or higher (case (b), next vehicle shifted away from the first) than the mean $\frac{a_i v_i}{\rho}$. The key remark here is that the two effects do not compensate for each other. On the one hand, distances shorter than the mean (case (a) in Fig. 4) do not improve the connectivity, as the individual vehicles were already within range when traveling at the mean speed and separated by the mean inter-arrival time. On the other hand, distances larger than the mean (case (b) in Fig. 4) can disrupt the link between two subsequent vulnerable vehicles, by creating a gap larger than R between them. As a result, the intrinsic variability of the road traffic metrics can only have a negative impact on the network connectivity, and considering average values means to overestimate the availability of V2V communication. A simple approach to address this issue is to introduce a factor $K \geq 1$ that reduces the propagation opportunities by multiplying the previous expression, which results[5] in a term $\frac{K a_i v_i}{\rho R}$.

Recall that the discussion above refers however to the case where vehicles all move in the same direction. The presence of an opposite vehicular flow can be accounted in a rough (yet effective, as we will show next) way, by considering a_i to be the average inter-arrival of vehicles at both ends of the bi-directional road segment. Finally, the carrier latency τ, as an application-level parameter, has no major impact[6] on the network connectivity expressed by $f(\cdot)$. In summary

$$s_i = v_i + \frac{R}{\tau}\, f\left(\frac{K\, a_i\, v_i}{\rho\, R}\right). \tag{3}$$

We still have to identify a proper expression for the function $f(\cdot)$ and a value for the parameter K. To that end, we employ the realistic dataset of road traffic on highways segments around Madrid that we presented in Sec. 4. By fitting the expression in (3) to network simulations of the worm propagation in such mobility datasets, we observed that a single function $f(x) = exp(-x^2)$ and a single value $K = 3$ fit the data for any combination of road traffic and communication parameters. The worm propagation speed along segment i is then

$$s_i = v_i + \frac{R}{\tau}\, exp\left[-\left(\frac{3\, a_i\, v_i}{\rho\, R}\right)^2\right]. \tag{4}$$

This single, simple expression can be employed to describe the average worm propagation speed along a road segment, given that its road traffic statistics, i.e., the average vehicular speed v_i and the average inter-arrival time a_i, are known. We remark that the exponential shape of $f(\cdot)$ and the rather high value of K make connectivity decrease very rapidly. E.g., when the average distance between two vehicles involved in the epidemics is half of the communication range, i.e., $\frac{\alpha_i v_i}{\rho_i} = \frac{R}{2}$, there is only a 10% probability that the worm can successfully propagate between the two.

We validate the per-road segment propagation model in (4) by assessing its capability of matching simulation results under the whole space of combinations of the system parameters R, ρ and τ. Fig. 5 compares the propagation speed s_i computed with the model in (4) against that obtained by running simulations on the Madrid highway datasets. We can observe that the model is consistently in good agreement with the simulation outcome, when varying any of R, τ, and ρ over their significant value ranges along the x axis. Moreover, we found this result to hold for any combination of highway segment, day time and weekday. in the Madrid dataset.

We also tested the model in (4) against simulations of the infection propagation along individual road segments of the Canton of Zurich scenario. We found again a good agreement between the model and the simulation, in Fig. 6. There, the plots marked as (a), (b) and (c) aggregate the results for all road segments that feature similar average vehicular speeds, ranging between 11 m/s (less than 40 km/h) and 28 m/s (over 100 km/h). Each plot displays a scatterplot of the worm propagation speed measured at each segment i, versus the road average inter-arrival time, a_i, with baseline parameters R = 100 m, τ = 1 s ρ = 1. The red curve represents the average behavior observed in simulation on all roads, while the black curve is the result provided by our model. The plots marked as (d), (e) and (f) show instead the worm propagation speed for different values of R, τ and ρ, respectively. There, for the sake of clarity, the scattered simulation samples are not shown and only the average curves, in red, are reported.

Overall, the results in Fig. 5 and Fig. 6 show that our data-driven model can faithfully mimic the average behavior of the worm propagation speed, under any road traffic condition, in both the Madrid and Canton of Zurich scenarios. Of course, the model does not capture the random variability around the mean that is observed for specific roads. This is due to the fact that we only consider the average values of v_i and a_i in our study, and not higher-order moments of their distributions.

5. As discussed later, we found K to be invariant to road traffic and communication settings, and we thus treat it as a constant in the following.

6. The only case where τ can indirectly affect the network connectivity is that of a carrier latency so large to be comparable to the time required to travel a whole road segment between two intersections. However, the latter is at least several tens of seconds, while τ is expected to be much shorter.

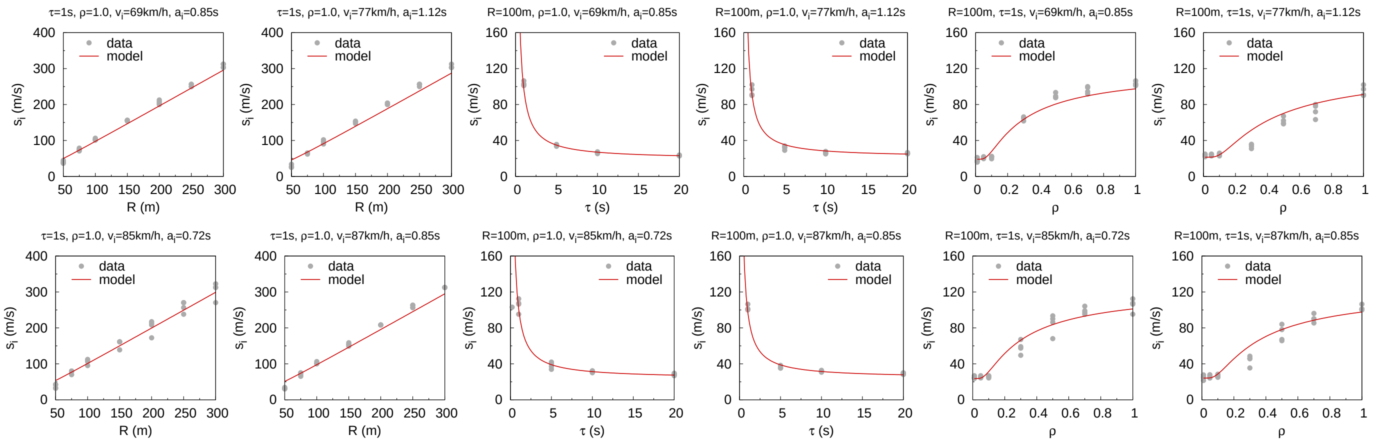


Fig. 5. Model validation. Per-road segment worm propagation speed in the Madrid highway datasets, from network simulations (dots) and as predicted by the proposed model (line), versus R (four leftmost plots), τ (four middle plots), and ρ (four rightmost plots). For each parameter, the four plots refer to a highway segment and day-time pair. Each plot gathers data from four weekdays yielding similar road traffic conditions (i.e., average speed and inter-arrival time).

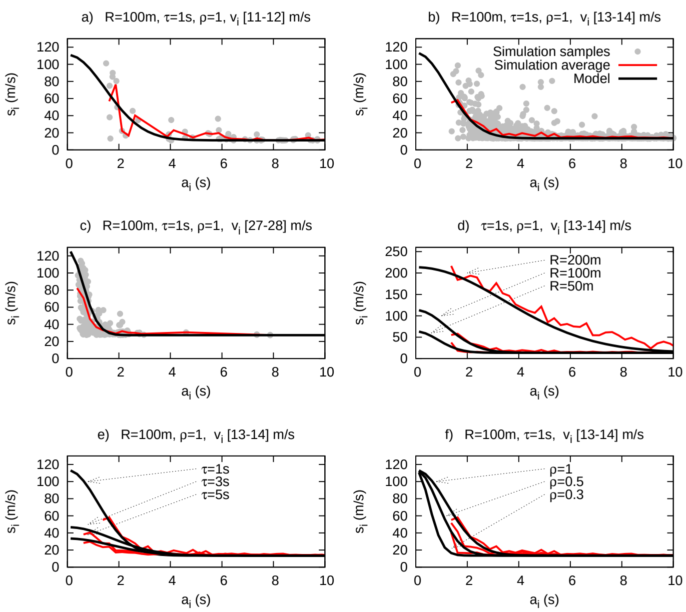


Fig. 6. Model validation. Per-road segment worm propagation speed versus the average inter-arrival time a_i in the Canton of Zurich dataset. Simulations, on individual roads (dots) and on average (red thin line), are compared to the proposed model (black thick line). Roads yielding similar average speed s_i are aggregated in plots (a,b,c). System parameters R, τ, and ρ are varied in plots (d,e,f).

This is an intentional choice that allows us to keep the model simple, and yet to obtain excellent results when considering the network-wide infection, as discussed next.

5.3 Road network-wide worm propagation

The per-road segment worm propagation speed expression in (4) can be leveraged to describe the propagation process over the whole road network. In particular, the road network-wide infection is completely described by the *spread delay*, i.e., the time that a worm takes to reach a specific location after the appearance of patient zero at the origin.

In order to translate the per-road segment propagation into the network-wide spread delay, let us represent the road layout as a graph G=$(\mathcal{V}, \mathcal{E})$, where the set of vertices $\mathcal{V}$ represents the intersections and the set of edges $\mathcal{E}$ represents the roads joining such intersections. Knowing the worm propagation speed s_i along a road segment i, as well as the length of such segment l_i, the spread delay from one end of the road to the other is immediately derived as w_i=$\frac{l_i}{s_i}$. Each edge in $\mathcal{E}$ can then be associated to a weight corresponding to its spread delay w_i. Note that the resulting weighted graph is time-varying, since the worm propagation speeds along each road change over time, and so do the weights derived from them.

Given the infection time t and the location on the road topology of patient zero, calculating the spread delay from the origin point to any other point of the region reduces to a single-source shortest path problem on the weighted graph associated to time t. A standard Dijkstra's algorithm can be used to efficiently solve the problem. The spread delay to a given location on the road network maps to the cost of the shortest path to its corresponding vertex or edge on the graph, or, in other words, to the sum of the spread delays along the fastest path from the infection origin to the given location.

An intuitive representation of the model accuracy is provided in Fig. 7. The plots depict the geographical spread of a worm originating in downtown Zurich at 3 pm, as occurring in simulation and as predicted by the model. The red dots represent the locations that are reached by both approaches at fixed times after the worm injection. Filled circles are used to denote locations reached in simulation only, and empty circles those reached by the model only. We can note that the worm propagation is almost identical in the two cases, as most of the reached points are covered at the same time by the simulation and the model. The differences, i.e., the points that are reached at each time instant by the simulation or by the model only, are few and always limited to the rim of the propagation process.

The spread delay for the epidemic process in Fig. 7 can be summarized in a plot such as that of Fig. 8(a). The plot portrays the road network-wide spread delay measured

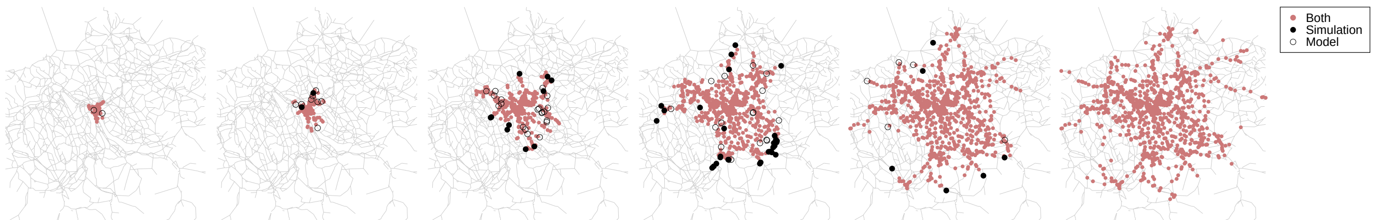
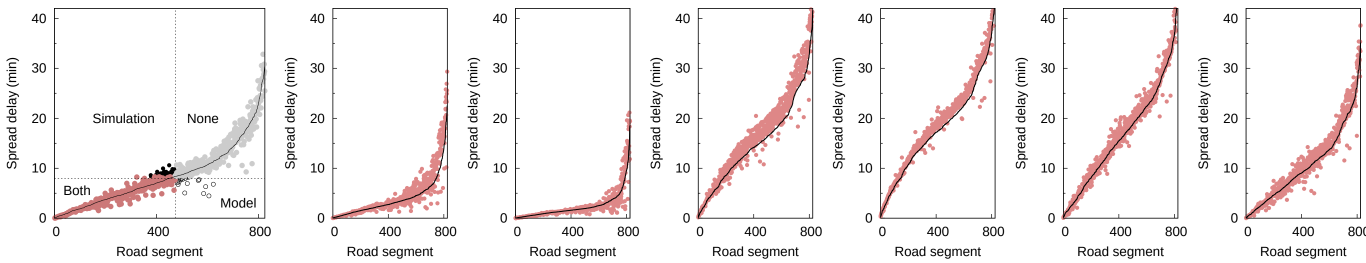


Fig. 7. Model validation. Geographical spread of the worm over the Canton of Zurich road network and at different time instants, in simulation (red dots and •) and in the proposed model (red dots and ○) with R = 100 m, τ = 1 s, ρ = 1.



(a) R = 100 m, τ = 1 s, ρ = 1 (b) $R = 200$ m (c) $R = 300$ m (d) $\tau = 5$ s (e) $\tau = 10$ s (f) $\rho = 0.3$ (g) $\rho = 0.7$

Fig. 8. Model validation. Road network-wide spread delay with (a) default settings, varying (b,c) R, (d,e) τ, (f,g) ρ.

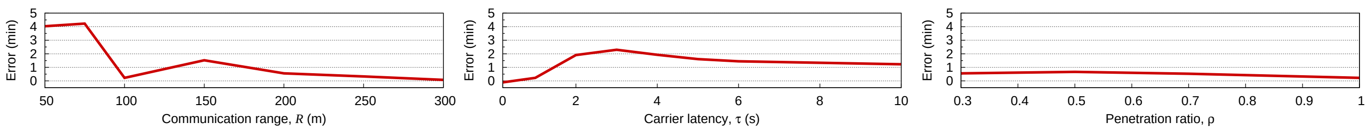


Fig. 9. Average error versus carrier communication range R (left), latency τ (middle) and penetration ratio ρ (right).

in simulation (dots), and that derived with our data-driven model (solid line). Graph vertices (i.e., road intersections) are ranked along the x axis according to the worm spread delay determined by the model. Therefore, by fixing a specific time instant along the y axis (e.g., 8 minutes in Fig. 8(a)), the plane is split into four regions. Dots in each region map to intersections that, 8 minutes after worm injection, are reached by infection (i) in both simulation and model, (ii) in simulation only, (iii) in model only, and (iv) in none of the two.

Clearly, it is desirable that the model solid line in Fig. 8(a) fits well the dots obtained in simulation. This is the case, as the deviation of the individual dots from the line is limited – which translates into the minor errors at the rim of the infection observed in Fig. 7. We remark that Fig. 8(a) refers to the case of R = 100 m, τ = 1 s, ρ = 1. However, the quality of the result is the same when the systems parameters R, τ, and ρ are varied, as shown in the other plots of Fig. 8.

Finally, a comprehensive picture of the model reliability in terms of road network-wide spread delay is provided in Fig. 9. The three plots show the average error, in minutes, between the simulation results and the model outcome for the whole parameter space. Notably, the error is always positive, i.e., the model always overestimate the speed of the infection. However, the error stays below 2 minutes for most of the combinations of R, τ and ρ, and is often at or below 1 minute.

6 Understanding the epidemics

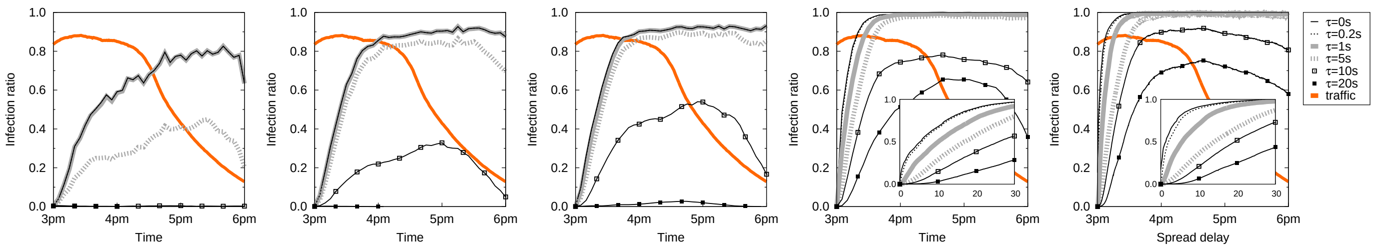
As a first step in the characterization of worm epidemics in large-scale vehicular networks, we aim at understanding the main features of the infection propagation, as well as the impact that the different system parameters have on it. To that end, we run a comprehensive simulation campaign in the Canton of Zurich scenario presented in Sec. 4.1. At this time, our focus is on on the worm infection propagation process in the vehicular environment. Thus, we do not consider patching as an option to recover or immunize the vehicles. In epidemiology, this is equivalent to consider a Susceptible, Infected (SI) model. We will study malware patching and the complete SIR with Immunization, in Sec. 7.

6.1 Worm carrier

We start by studying the impact of the worm carrier. Let us for now assume that patient zero appears in downtown Zurich, i.e., at the center of the map in Fig. 2(a) approximately, at 3 pm, when the road traffic intensity is at its peak. In Fig. 10(a), we focus on the carrier mechanism, setting the carrier latency τ = 1 s and comparing the results achieved by a broadcast carrier against those obtained by a unicast carrier. The reach of the epidemics is measured in terms of the *infection ratio*, i.e., the fraction of vulnerable vehicles that the worm has reached four hours after the injection time[7]. The x axis reports the combined V2V technology and security flaw penetration ratio ρ, growing from 1% to 100% of the vehicles.

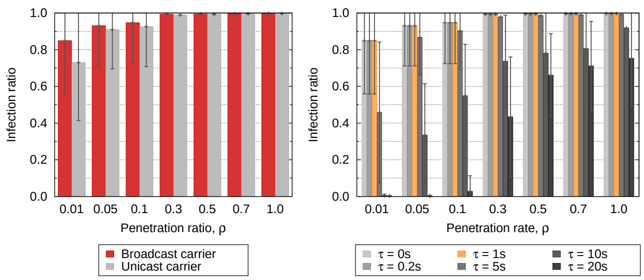
We observe that a broadcast carrier achieves a higher infection ratio than a unicast one. This is expected, since the latter mechanism requires the worm to carry out multiple self-propagations, each taking a time τ, to reach all the nodes that a broadcast-carrier worm can infect with a single self-propagation in a time τ. However, the difference is marginal

7. As we will later see, such a timespan is largely sufficient for this analysis.



(a) ρ = 0.01 (b) ρ = 0.05 (c) ρ = 0.1 (d) ρ = 0.5 (e) ρ = 1.0

Fig. 11. Infection ratio versus time, for different penetration ratios ρ and latencies τ, in presence of a broadcast carrier.



(a) Carrier mechanism (b) Carrier latency, τ.

Fig. 10. Infection ratio versus the penetration ratio ρ, in presence of different worm carrier features. Error bars represent the standard deviation. (a) Broadcast or unicast carrier. (b) Carrier latency. Figure best viewed in color.

at very low penetration ratios, and the two carrier mechanisms perform basically the same once 5% or more of the vehicles are susceptible of contracting the worm.

As far as the impact of ρ is concerned, higher penetration ratios clearly lead to a more connected network of vulnerable vehicles, which in turn facilitates the spreading of the worm. A value of $\rho = 0.3$, mapping to 30% of communication-enabled vehicles, is already sufficient for the worm to achieve a complete infection of the vehicular network. However, it is surprising to note that very high infection ratios, well above 0.7, are achieved even in very sparse networks comprising 1% of the cars, and that 90% of the network is reached by the worm when just 5% of the vehicles are vulnerable. This susceptivity of vehicular environments to worm epidemics is imputable to the fact that the high velocity of cars can compensate for the reduced penetration ratio, generating many V2V contacts and facilitating the worm self-propagation in a store-carry-and-forward fashion.

In Fig. 10(b), we focus on the broadcast carrier case and study the impact of the carrier latency τ, in presence of different penetration ratios. More precisely, we consider a τ ranging from 0 s (which represents an ideal upper bound to the worm spreading performance, since the worm infection is instantaneous) to 20 s. We observe that, even in presence of low penetration ratios, a sufficiently fast worm (i.e., one capable of self-propagating to its 1-hop neighborhood in one second or less) can successfully infect the vast majority of the vehicles in a very large region such as the one we considered. In fact, when $\tau \leq 1$ s, at least 85% of the vehicles are infected under any penetration ratio. Longer carrier latencies appear instead to be more dependent on ρ: when $\tau \geq 10$ s the worm is unable of spreading throughout the whole network even if all the vehicles are susceptible of being infected.

The results above let us conclude that: (i) unicast-carrier worm are as dangerous as broadcast-carrier ones; (ii) a low percentage of vulnerable vehicles is sufficient for worms to spread over a large area, due to the fast dynamics of road traffic that facilitate malware propagation; (iii) worms do not need to be extremely fast in infecting neighboring vehicles, as a 1-second carrier delay[8] is largely sufficient to vehiculate the worm to the whole network in all conditions.

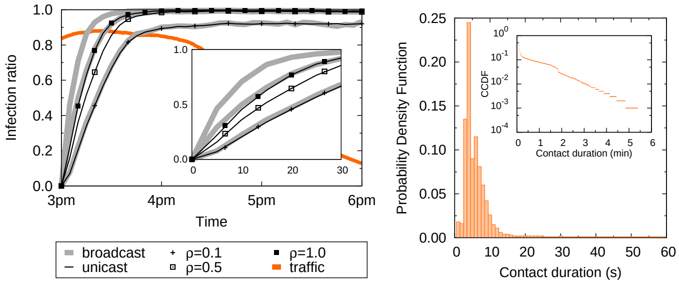
6.2 Worm epidemics over time and survivability

The percentages of infected nodes presented before are computed at some fixed temporal deadline. Now, we consider the temporal dynamics of the infection propagation. Specifically, we focus on: (i) the time needed for the worm to reach a given infection ratio within the vehicular network; (ii) the so-called *worm survivability*, defined as the period of time during which the infection can persist in the vehicular network.

6.2.1 Results

In Fig. 11, each plot refers to a specific penetration ratio ρ, and portrays the temporal evolution of the infection for different values of the carrier latency τ. When $\rho = 0.01$, in Fig. 11(a), only rapid malware with carrier latencies τ of 1 s or less can propagate through most (although not all) of the network. The bell-shaped infection ratio for $\tau = 5$ s is explained by the aggregated road traffic volume, also depicted in the figure as the thick solid orange line: the worm is not fast enough to infect the whole network before the traffic peak ends, at around 4.30 pm, i.e., 1 hour 30 minutes after the infection started. As a result, the infection stays limited to the surroundings of the injection area, and then dies out when the traffic becomes sparser due to vehicles leaving the area or concluding their trips. Slower worms do not even start to spread in the system. Increasing ρ to 0.05, in Fig. 11(b), also allows slightly slower worms, characterized by a τ in the order of a few seconds, to infect an even larger majority of the vehicles. Namely, worms with $\tau \leq 5$ s perform similarly and achieve a 95% infection ratio with a linear growth during the first 45 minutes from the worm injection. This clearly makes such worms extremely dangerous, since, in order to be effective, a patch should be provided to network nodes within a very few minutes after the worm injection. The bell shape now characterizes the diffusion

8. We remark that 1 s is a perfectly realistic value for the carrier latency, considering that worms consists in a few tens of KB of code and that the V2V base data transmission rate is in the order of a few Mbps.



(a) Carrier mechanism (b) V2V contact duration

Fig. 12. (a) Infection ratio versus time, for different carrier mechanisms and penetration ratios ρ. (b) V2V contact duration distribution in the Canton of Zurich scenario.

of malware with a carrier latency of 10 s, for the same reasons discussed above. Slower worms find it still difficult to spread at such a low ρ.

A larger participation of 10% of the cars in the network, in Fig. 11(c), does not affect the behavior of worms characterized by a $\tau \leq 5$ s, and only slightly favors slower worms. On the other hand, as the population of susceptible vehicles grows to 50% of the overall road traffic, in Fig. 11(d), we remark two effects. First, the infection evolutions of the faster worms start to separate. This effect is highlighted in the inset plot, which details the spreading process during the first 30 minutes from the worm injection time. Indeed, very fast worms (i.e., with $\tau < 1$ s) were previously limited by the lack of multi-hop connectivity, and had to rely on carry-and-forward to find new susceptible vehicles. As a result, their performance, hitting the bar imposed by the limited network connectivity, was similar to that of slower worms (e.g., with $\tau = 5$ s). Now, fast malware can take advantage of the presence of larger connected clusters of vehicles, and spread over 95% of the network in some 20 minutes. Moreover, the growth is now faster than linear, with 50% of the nodes being infected in less than 6 minutes. As a second remark, the higher penetration ratio has a largely beneficial effect on the spread dynamics of slower worms, as now even the curves for $\tau \geq 10$ s depict the infection of very wide portions of the network. However, the worm still does not self-sustain in those conditions, since its infection ratio tends to drop once the road traffic peak ends.

In Fig. 11(e) we consider the case where all the vehicles are communication-enabled, i.e., the best possible network connectivity scenario. The effects already observed in the previous plot are exacerbated, as the faster worms infect 50% of the network in less than 2 minutes and spread over 95% of nodes in 10 minutes. Slower worms also take advantage of the increased connectivity, although they do not achieve complete infection ($\tau = 5$ s) or even self-sustainability ($\tau \geq 10$ s).

A similar temporal analysis can be done when comparing different carrier mechanisms. Fig. 12(a) depicts the infection evolution of broadcast and unicast worms, in presence of varying penetration ratios, when $\tau = 1$ s. The inset plot shows again the detail of the first thirty minutes of the spreading process. We can note that, although they attained a similar final infection ratio in Fig. 10(a), unicast and broadcast carriers differ in terms of delay. In fact, the difference is only remarkable at high penetration ratios, when $\rho = 0.5$ or 1. As the penetration ratio decreases, the difference in the time needed to infect the network becomes negligible, and the two paradigms match when 10% or less of the cars are involved.

6.2.2 Carrier latency and contact time

The previous results show a striking difference in the spread process of worms characterized by various carrier latencies. In particular, values of τ of 1 s or less seem to result in high infection ratios no matter the number of vehicles involved in the network; moreover, such values of τ allow the infection to occur much faster as the penetration ratio increases. On the other hand, worms with a $\tau \geq 10$ s need high penetration ratios to propagate and take a lot of time in doing so. Values of τ in between those result in intermediate behaviors.

The physical reason behind this diversity lies in the V2V contact duration distribution, shown in Fig. 12(b). There, we can observe that most contacts among moving vehicles are extremely short-lived: more than 70% last less than 5 seconds, and less than 10% are longer than 10 seconds. Indeed, the vast majority of links is established by high-speed vehicles moving in opposing directions along highways in the Canton of Zurich scenario: these links last just a few seconds and dominate the network connectivity dynamics. We can remark that relatively long-lived contacts are also present, but they decay exponentially fast as per the inset plot in Fig. 12(b). As a result, only 5% of the links last one minute or more, making their contribution to the overall vehicular network connectivity of lesser importance with respect to short contacts.

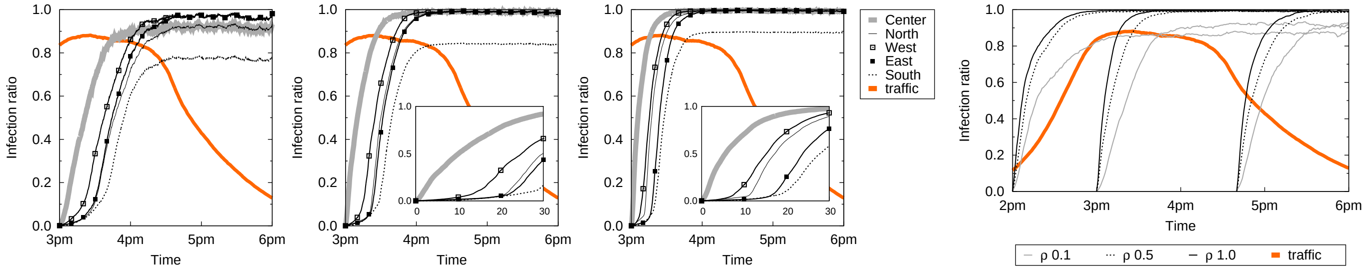
Our conclusion is that fast worms, capable to spread from one vehicle to another in one second or less, can exploit any contact occurring in the network. Conversely, a worm characterized by a τ of 5 s will be only able to leverage 20% of the contacts, and one with $\tau = 10$ s will propagate through a mere 8% of the actual V2V links. In other words, fast worms enjoy a more connected network to spread through.

6.3 Infection origin

The previous results all refer to the case where the worm is injected in the center of the geographical region we consider, which corresponds to the urban area of Zurich. Moreover, we considered the the infection start at the beginning of the afternoon traffic peak, occurring at 3 pm. Given the fast spatiotemporal dynamics of road traffic, the origin of the infection is a critical aspect to be taken into account. Here, we study the impact that the location and hour at which the worm is first injected in the vehicular network have on the infection propagation.

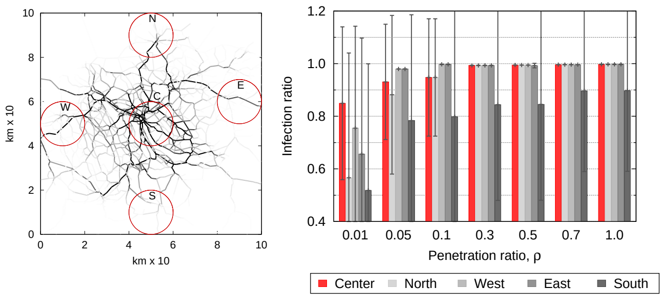
6.3.1 Patient zero location

We first vary the worm origin area, by considering five different possibilities. Other than at the city of Zurich, i.e., our default setting, we analyze infections starting at the North, West, South and East boundaries of the 10.000-km^2 simulated region. More precisely, as plotted in Fig. 13(a), we identify one circular area for each origin location and pick, at each simulation run, one vehicle in that area as our patient zero.



(a) ρ = 0.1 (b) ρ = 0.5 (c) ρ = 1.0 (d) Injection time

Fig. 14. Infection origin. (a,b,c) Infection ratio versus time, for different patient zero locations and penetration ratios ρ. (d) Infection ratio versus time, for different worm injection times and penetration ratios ρ.



(a) Location map (b) Infection ratio

Fig. 13. Infection origin. (a) Map of the possible patient zero locations. (b) Infection ratio versus the penetration ratio ρ, for each patient zero location in the map.

The overall infection ratio recorded for each origin location, under different penetration ratios, is shown in Fig. 13(b). Clearly, the position of the worm injection plays a major role in the success of the spreading: placing patient zero in the West or East areas yields an infection ratio comparable, and at times even better, than that achieved in the Center case. Conversely, worms starting from the North area seem to be slightly penalized, and those injected in the South area consistently lag behind the other cases.

The explanation to such a result lies in the heterogeneity of the road topology, composed of highways, major arterial and minor urban or suburban roads, that are characterized by diverse car traffic densities. This can be observed in Fig. 13(a), where roads are colored according to the daily traffic volume they carry: darker roads are more trafficked, while a very few vehicles travel over roads that are almost white, and thus hardly visible in the plot. The resulting map outlines how most of the vehicles travel in or around the city of Zurich, but also that the West and East areas are traversed by major highways. The North area is also touched, although in a smaller measure, by heavy-traffic arteries, whereas the South area appears only characterized by low-traffic roads. It is easy to conclude that, even in presence of high penetration ratios, worms injected in the South area hardly find vehicles to carry them towards the rest of the region.

The infection survivability in presence of different patient zero locations and penetration ratios is depicted in Fig. 14(a), Fig. 14(b), and Fig. 14(c). As already observed, higher penetration ratios allow for a faster diffusion of the infection, an effect that does not seem affected by the injection location.

Interestingly, the plots show that an infection starting at the Center area is significantly faster than those starting at the region borders. The difference lies in the first phases of the infection. When the infection starts from the Center, the infection ratio has a linear (or super-linear at high penetration ratios) growth, while the curves for worms injected at the region borders are very slow at first. More precisely, in the North, West, South and East cases the infection ratio stays close to zero up to a specific point, where the spreading process seems to ignite and a linear (or super-linear at high penetration ratios) growth, similar to that of the Center case, begins. The precise moment at which such a transition occurs varies for each injection area, and appears the earliest in the West case and the latest in the South case. It is intuitive to map the transition point to the instant when the worm reaches the urban area of Zurich. Such a point corresponds to the injection time for the Center area, while it depends on how easily the worm can travel to the city center in the other cases: e.g., the presence of a heavy-traffic highway clearly speeds up infections originating in the West area.

6.3.2 *Worm injection time*

The road traffic has temporal variations, and it is typically heavier at peak hours in the morning and in the afternoon. This motivates a study of the impact of the injection time. We thus fix the patient zero location within the Center area, and vary the time at which the first infected vehicle appears. Fig. 14(d) illustrates the resulting infection ratio over time, under different penetration ratios. It can be observed that, no matter the penetration ratio considered, the injection time does not seem to have any significant effect on the overall infection ratio achieved by the vehicular worm, nor on its survivability. Instead, the injection time has a non-negligible impact on the latency of the epidemics: a patient zero appearing during the rush hours, e.g., at 3 pm, induces a faster infection, thanks to the denser and thus better connected vehicular network that is available at that moment of the day. Injecting the worm at the same location, but during off-peak hours, results in a slower propagation, consistently with the sparser car traffic observed at those times.

6.4 Summary

Summarizing our findings, we conclude that a reasonably fast worm can be extremely dangerous, independently of the carrier mechanisms it adopts, of the susceptible vehicle penetration, or of the infection process origin. More precisely, we observed that a worm that fits in a few IP packets, and that can thus be transmitted over the wireless medium in less than one second (accounting for channel contention and losses), can easily infect a vast majority of the tens of thousands of vehicles traveling in a very large region. Even worse, such infection would occur in a time in the order of a few tens of minutes at most, making it hard to counter the infection.

The physical reasons behind such an impressive performance of the worm diffusion lie in (i) the elevate mobility of nodes in the vehicular network, and (ii) the high number of short-lived connections generated by the movement of vehicles. Both these factors contribute in creating an ideal environment for a fast worm to self-propagate. We also found the geographical location of the infection origin to have a dramatic effect on the reach and speed of the epidemics, mainly due to the spatial heterogeneity of road traffic. The temporal heterogeneity of road traffic is instead the cause behind the different infection latencies observed when varying the injection time of patient zero in the system.

7 Exploiting the epidemics model

In this section, we leverage the proposed model of a vehicular worm epidemics in order to derive results that would be computationally infeasible via network simulation. Specifically, in Sec. 7.1 we use the model to perform a complete fine-grained analysis of the level of danger associated to infections that originate at each geographical location in the Canton of Zurich scenario. Then, in Sec. 7.2, we exploit the model to design a patching strategy aimed at taming vehicular worm epidemics.

7.1 Danger analysis of patient zero location

In Sec. 6.3, we discussed the relevance of the origin location to the spread and rapidity of the infection process. However, that analysis was limited to worms injected at random locations within five broad regions, due to the cost of running more extensive simulations of the epidemics.

The numerical model we presented in Sec. 5 lets us delve much deeper in the study of the impact of patient zero's location. Specifically, the very low computational complexity of the model allows us to estimate the evolution of the vehicular worm epidemics when it originates on each of the hundreds of roads present in the 10.000-km^2 region of the Canton of Zurich. We can thus draw a complete map of the dangerousness of each geographical location as the infection origin, in Fig. 15(a). There, we color each road segment according to the spread delay that a worm injected in that segment would require in order to infect 95% of the susceptible vehicular population.

The map shows that the infection origins that are more dangerous, i.e., yield lower spread delays, are those inside the city of Zurich – a result consistent with the discussion in Sec. 6.3. However, we have now a more comprehensive view of the system, and we can observe how the spread delay grows (and thus the epidemics become less rapid) as we move away from the city center. Interestingly, the reduction is not geographically uniform: we remark that, e.g., low-delay regions stretch towards the West, and, to a lesser extent, towards the South and North-East.

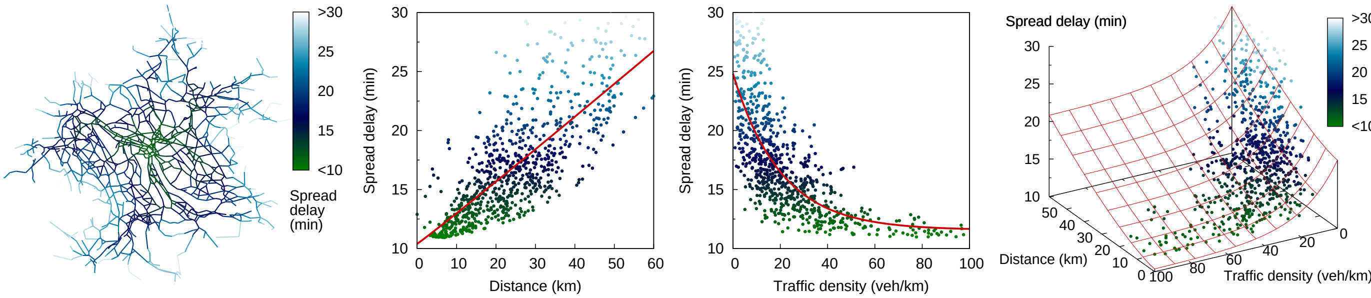
In order to clarify the reasons behind the geographical heterogeneity observed in the map, we investigate the correlation between the spread delay associated to each road segment and two sensible measures: (i) the distance of the segment from the center of the city of Zurich, in Fig. 15(b), and the average traffic density measured on the segment, in Fig. 15(c).

We remark a positive linear correlation between the distance from Zurich and the spread delay in Fig. 15(b). However, there is also significant variability in the numerical data around the linear fitting, which confirms our obervation that the distance from the city center alone cannot be the only physical factor driving the level of danger associated to a geographical location. In Fig. 15(c), the vehicular traffic is negatively correlated to the spread delay, meaning that roads with more intense traffic are more dangerous locations where to start the infection. Moreover, we observe that such a negative correlation is exponential, i.e., a minor growth in troad traffic intensity tends to induce a significant decrease of the spread delay. The reason is that heavily trafficked roads are typically linked to each other, and build a well-connected vehicular network backbone through which a worm can easily propagate. Still, even in Fig. 15(c) the data is quite sparse around the negative exponential fitting, and the density information alone is again not sufficient to explain the map.

However, by considering the two measures at once, a bi-dimensional fitting $\sigma(\Delta, T) = a + b\Delta^c + de^T$ is possible, where σ is the spread delay, Δ is the road segment distance from the center of Zurich, T is its average traffic density, and a, b, c, d, e are constants. Such a joint fitting with $a = 10.3$, $b = 0.03$, $c = 1.4$, $d = 8.7$, $e = 1.05$, depicted in Fig.15(d), approximates the spread delay with a limited Root Mean Square error of 2.19 minutes. This good result lets us conclude that the dangerousness of a location can be well characterized by jointly considering its distance from the city center and its average traffic density.

7.2 Containing the worm epidemics

The results in Sec. 6 unveiled the dangerousness of vehicular worms, which motivates the development of solutions for the rapid containment of their outbreaks. Assuming the SIR with Immunization model introduced in Sec. 3.3, the typical techniques proposed in the literature are preemptive immunization and interactive patching [20], [21]. In the first case, a subset of the vehicles is preemptively immunized so as to prevent the propagation of the worm. However, preemptive immunization makes sense only in the case of static networks, where immunized nodes can disrupt the connectivity exploitable by the malware. In highly mobile environments, worms can easily overcome the obstacle of preemptively immunized vehicles thanks to car movements. In the case of interactive patching, a patch to the worm is released in the network and diffused through V2V communication in an epidemic fashion. In other words, the patching follows a spreading process similar to that of the worm itself. However, resorting to V2V communication



(a) Geographical map (b) Distance (c) Road traffic density (d) Joint

Fig. 15. Spread delay to infect 95% of the susceptible population from each road in the Canton of Zurich. (a) Geographical map. (b) As a function of the distance to the center of Zurich. (d) As a function of the average road traffic density. (e) As a joint function of the two measures before.

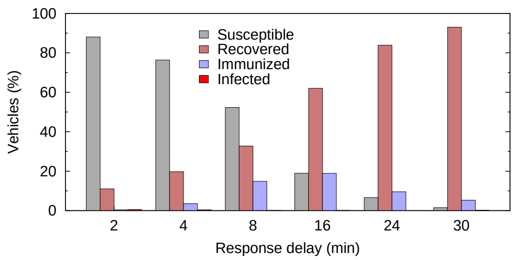


Fig. 16. Smart cellular patching via the proposed model.

to contain the malware epidemics does not seem a sensible choice, as it implies high delays and cannot guarantee the complete removal of the threat.

We consider instead that cellular communication can be leveraged to distribute the patch in a rapid and reliable fashion. Indeed, vehicles already start to be equipped with 3G/4G radios, whose diffusion will anticipate that of V2V communication interfaces. Therefore, that of a complete cellular coverage of V2V-enabled vehicles seems a reasonable assumption. The problem then becomes that of determining which vehicles to patch. If a rough estimation of the area and time at which the infection started is available, a *smart cellular patching* can be adopted, limiting the immunization to vehicles actually interested by the infection.

We thus propose a smart cellular-based patching based on our data-driven model of the worm epidemics. Namely, the model is exploited to determine the region within which the worm may have spread since the estimated infection instant. Then, only vehicles within such a region are immunized through the cellular network. We remark that an equivalent network simulation would take hours: given the rapidity of the epidemics, the simulation result would be already outdated at the time it becomes available.

Fig. 16 shows the results of the smart patching in the Canton of Zurich, considering that the epidemics starts in the center of Zurich at the peak traffic time. This is a worst-case scenario, since it yields maximum network connectivity and thus ideal conditions for the vehicular malware to self-propagate. The *response delay* is the estimated time between the patient zero appearance and the instant at which the smart patching is run: clearly, longer response delays imply that the infection has already reached larger portions of the road network when countermeasures are taken. For each value of the response delay (along the x axis) we report the number of vehicles belonging to different and mutually exclusive categories: *susceptible* nodes were not infected and did not receive the patch, *recovered* nodes were infected and later recovered upon receiving the patch through the cellular network, *immunized* nodes were not infected yet received the patch, and *infected* nodes were infected but did not received the patch. Clearly, the goal of a smart cellular-based patching is to recover all infected nodes, leaving no infected vehicles and reducing the number of unnecessarily immunized nodes to a minimum.

The results show that for a response time of 2 minutes, the model correctly predicts the nodes to be patched, with a negligible number of unnecessarily immunized vehicles. As the response delay increases, the percentage of vehicles infected by the malware grows, leading to the necessity of patching a larger portion of the road traffic. Yet, our model allows to successfully patch all infected vehicles, sparing up to 90% of transmissions with respect to an undiscerning patching, and limiting the percentage of unnecessarily immunized nodes to 20% in the worst case. More importantly, in all cases no node remains infected after the smart patching, which proves once more the quality of the model and its applicability to the efficient containment of malware outbreaks.

8 Conclusions

We presented an extensive study of malware epidemics in vehicular networks through V2V communication. Our simulative analysis evidenced the high level of danger of vehicular worms, capable of spreading through very large areas and infect tens of thousands of vehicles in a tens of minutes at most. We found that the high mobility of vehicular nodes and the elevate number of short-lived V2V contacts they generate are the key reason behind such a result. We then presented a simple yet very effective data-driven model of the worm propagation process, and leveraged it to show that the level of danger associated to the worm injection position can be ascribed to the distance of the location from the urban center and to the local road traffic density. We also employed the model as part of a solution for the containment of the epidemics, based on smart patching of infected vehicles through cellular communication.

REFERENCES

[1] O. Trullols-Cruces, M. Fiore, J.M. Barcelo-Ordinas, *"Understanding, Modeling and Taming Mobile Malware Epidemics in a Large-scale Vehicular Network"*, IEEE WoWMoM, Madrid, Spain, 2013.

[2] P. Ferrie, P. Szor, R. Stanev, R. Mouritzen, *"Security responses: Symbos.cabir"*, Symantec Corporation, 2004.

[3] E. Chien, *"Security response: Symbos.mabir"*, Symantec Corp., 2005.

[4] M. Lactaotao, *"Security information: Virus encyclopedia: Symbos comwar.a: Technical details"*, Trend Micro Incorporated, 2005.

[5] J. Kleinberg, *"The wireless epidemic"*, Nature, 449, 2007

[6] E. Anderson, K. Eustice, S. Markstrum, M. Hanson, P. Reiher, *"Mobile Contagion: Simulation of Infection & Defense"*, Symp. on Measurement, Modelling, and Simulation of Malware, Monterey, USA, 2005.

[7] J. Su, K.W. Chan, A.G. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara, A. Goel, *"A Preliminary Investigation of Worm Infections in a Bluetooth Environment"*, ACM WORM, Fairfax, VA, USA, 2006.

[8] P. Akritidis, C.W. Yung, V.T. Lam, S. Sidiroglou, K.G. Anagnostakis, *"Proximity Breeds Danger: Emerging Threats in Metro-area Wireless Networks"*, USENIX Security, Boston, MA, USA, 2007.

[9] P. Wang, M.C. Gonzalez, C.A. Hidalgo, A.-L.Barabasi, *"Understanding the spreading patterns of mobile phones viruses"*, Science 324, 2009.

[10] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, A. Nucci, *"A Social Network Based Patching Scheme for Worm Containment in Cellular Networks"*, IEEE INFOCOM, Rio de Janeiro, Brasil, 2009.

[11] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, *"Experimental Security Analysis of a Modern Automobile"*, IEEE S&P, Oakland, CA, USA, 2010.

[12] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, I. Seskar, *"Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study"*, USENIX Security, Washington, DC, USA, 2010.

[13] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, *"Comprehensive Experimental Analyses of Automotive Attack Surfaces"*, USENIX Security, San Francisco, CA, USA, 2011.

[14] P.E. Ross, *"A Cloud-Connected Car Is a Hackable Car, Worries Microsoft"*, IEEE Spectrum, 2014.

[15] A. Mizroch, *"The Dangers of the Cloud: Planes, Automobiles... and Wearables"*, Wall Street Journal, 2014.

[16] Reuters, *"Obama Backs Highway Fund Fix, Touts 'Talking' Cars"*, The New York Times, 2014.

[17] C. Miller, C. Valasek, *"A Survey of Remote Automotive Attack Surfaces"*, Black Hat, Las Vegas, NV, USA, 2014.

[18] B. Parno, A. Perrig, *"Challenges in securing vehicular networks"*, HotNets-IV, College Park, MD, USA, 2005.

[19] M.N. Mejri, J. Ben-Othman, M. Hamdi, *"Survey On VANET security challenges and possible cryptographic solutions"*, Vehicular Communications, 1(2), 2014.

[20] S.A. Khayam, H. Radha, *"Analyzing the Spread of Active Worms over VANET"*, ACM VANET, Philadelphia, PA, 2004.

[21] M. Nekovee, *"Modeling the Spread of Worm Epidemics in Vehicular Ad HocNetworks"*, IEEE VTC-Spring, Melbourne, 2006.

[22] L. Cheng, R. Shakya, *"VANET Worm Spreading from Traffic Modeling"*, IEEE RWS, New Orleans, LA, USA, 2010.

[23] M. Gramaglia, P. Serrano, J.A. Hernandez, M. Calderon, C.J. Bernardos, *"New Insights from the Analysis of Free Flow Vehicular Traffic in Highways"*, IEEE WoWMoM, Lucca, Italy, 2011.

[24] J. Wang, Y. Liu, K. Deng, *"Modelling and simulating worm propagation in static and dynamic traffic"*, IET Int. Transport Systems, 8(2), 2014.

[25] H. Wu, R. Fujimoto, R. Guensler, M. Hunter, *"MDDV: a mobility-centric data dissemination algorithm for vehicular networks"*, ACM VANET, Philadelphia, USA, 2004.

[26] J. Zhao, G. Cao, *"VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks"*, IEEE INFOCOM, Barcelona, Spain, 2006.

[27] C. Barberis, G. Malnati, *"Epidemic Information Diffusion in Realistic Vehicular Network Mobility"*, ICUMT, St.Petersburg, Russia, 2009.

[28] Y.P. Fallah, C.-L. Huang, R. Sengupta, H. Krishnan, *"Analysis of Information Dissemination in Vehicular Ad-Hoc Networks with Application to Cooperative Vehicle Safety Systems"*, IEEE Trans. Vehicular Technology, 60(1), 2011.

[29] A. Agarwal, D. Starobinski, T.D.C. Little, *"Analytical Model for Message Propagation in Delay Tolerant Vehicular Ad Hoc Networks"*, IEEE VTC-Spring, Singapore, 2008.

[30] E. Baccelli, P. Jacquet, B. Mans, G. Rodolakis, *"Information propagation speed in bidirectional vehicular delay tolerant networks"*, IEEE INFOCOM, Shanghai, China, 2011.

[31] H. Wu, R.M. Fujimoto, G.F. Riley, M. Hunter, *"Spatial Propagation of Information in Vehicular Networks"*, IEEE Trans. Vehicular Technology, 58(1), 2009.

[32] Z. Zhang, G. Mao, B.D.O. Anderson, On the Information Propagation Process in Mobile Vehicular Ad Hoc Networks IEEE Trans. Vehicular Technology, 60(5), 2011.

[33] N. Weaver, V. Paxson, S. Staniford, R. Cunningham, *"A Taxonomy of Computer Worms"*, ACM WORM, Washington, DC, USA, 2003.

[34] B. Raney, N. Cetin, A. Völlmy, M. Vrtic, K. Axhausen, K. Nagel, *"An agent-based microsimulation model of Swiss travel: First results"*, Networks and Spatial Economics, 3(1), 2003.

[35] Y. Pigne, G. Danoy, P. Bouvry, *"A Vehicular Mobility Model based on Real Traffic Counting Data"*, Nets4Cars, Oberpfaffen, Germany, 2011.

[36] S. Uppoor, O. Trullols-Cruces, M. Fiore, J.M. Barcelo-Ordinas, *"Generation and Analysis of a Large-scale Urban Vehicular Mobility Dataset"*, IEEE Transactions on Mobile Computing, 13(5), 2014.

[37] L. Zhang, J. Ahn, B. Krishnamachari, F. Bai, *"Optimizing Content Dissemination in Heterogeneous Vehicular Networks"*, PATH/Tsinghua Workshop on ITS, 2010.

[38] J. Yuan, Y. Zheng, X. Xie, G. Sun, *"Driving with knowledge from the physical world"*, ACM SIGKDD, San Diego, CA, USA, 2011.

[39] M. Doering, T. Pögel, W.-B. Pöttner, L. Wolf, *"A new mobility trace for realistic large-scale simulation of bus-based DTNs"*, ACM CHANTS, Chicago, IL, USA, 2010.

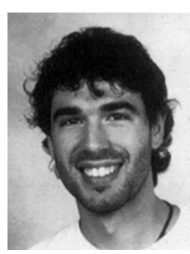
[40] M. Gramaglia, O. Trullols-Cruces, D. Naboulsi, M. Fiore, M. Calderon, *"Vehicular Networks on Two Madrid Highways"*, IEEE SECON, Singapore, 2014.

[41] F. Bai, D. D. Stancil, and H. Krishnan, *"Toward understanding characteristics of dedicated short range communications (DSRC) from a perspective of vehicular network engineers"*, ACM MobiCom, Chicago, IL, USA, 2010.

[42] F. Martelli, M. E. Renda, G. Resta, and P. Santi, *"A measurement-based study of beaconing performance in IEEE 802.11p vehicular networks"*, IEEE INFOCOM, Orlando, FL, USA, 2012.

[43] G. Leduc, *"Road Traffic Data: Collection Methods and Applications"*, European Commission Joint Research Centre Technical Notes, 2008.

Oscar Trullols-Cruces (S'09) is a Research Engineer at Universitat Politècnica de Catalunya (UPC) He received his PhD from UPC, in 2014, and M.Sc and B.Sc degrees from UPC, in 2008. He joined the Computer Architecture Department in 2007 with the Computer Networking Research Group. He visited KTH, Stockholm, Sweden, in 2009. His research interests include Internet of things, mobile ad hoc networks, delay tolerant networks and mobility modeling.



Marco Fiore (S'05, M'09) is a researcher at CNR-IEIIT, Italy, and an associate researcher at Inria, France. He received a PhD degree from Politecnico di Torino, in 2008, and a habilitation à diriger des recherches (HDR) from University of Lyon, in 2014. He was an associate professor at INSA Lyon, France, and a visiting researcher at Rice University, USA, and Universitat Politecnica de Catalunya, Spain. His interests are on mobile traffic analysis and vehicular networking.

Jose M. Barcelo-Ordinas (M'04) is an Associate Professor at Universitat Politècnica de Catalunya (UPC). He received his PhD and M.Sc at UPC (1998 and 1991). He joined the CompNet research group in 1993. He has participated in several European projects such as EXPLOIT, BAF, EXPERT, NETPERF, MOEBIUS, WIDENS projects, and EuroNGI, EuroNFI and EuroNF (VII FP) Networks of Excellence (NoE). His currently research areas are Mobile Networks, VANETs and Wireless Sensor Networks.