Blocking Epidemic Propagation in Vehicular Networks

Pavlos Basaras*and Ioannis Belikaidis*, Leandros Maglaras‡, Dimitrios Katsaros*†
*Department of Electrical & Computer Engineering, University of Thessaly, Greece
†Department of Electrical Engineering & Yale Institute for Network Science, Yale University
‡Computer Science & Informatics, De Montfort University, Leicester, UK
{pabasara,iobelika,dkatsar}@inf.uth.gr, leandros.maglaras@dmu.ac.uk

***Abstract*—The propagation of software viruses over a vehicular network where vehicles communicate via V2V links can have disastrous effects for the vehicles themselves and the ad hoc network. Here, we propose a simple distributed solution to block virus spreading over a VANET by initiating a negating spreading process that informs vehicles for the presence of infected nodes. We evaluate the proposed approach via simulations using established simulators, and show that the method can significantly limit the percentage of vehicles infected by the virus.**

I. Introduction

The introduction in the automotive market of vehicles with wireless communication capabilities that will allow a vehicle to communicate with other vehicles in vicinity (vehicle-to-vehicle communication, V2V) will bring a revolution in sectors such as vehicle/driver safety [1], Internet access and entertainment [2]. V2V systems are particularly appealing for the vision of the "always connected car", because a fully functional V2V system would connect drivers traveling near each other, allowing a vehicle to accumulate information about what other vehicles are doing even if the driver can not see them. The prospects of this technology is truly tremendous, from practically eliminating human casualties, to reducing traffic congestion, or setting up vehicular computing clouds to exploit the aggregate computing and storage capability of roaming cars. NHTSA estimates that this technology can prevent up to $592,000$ crashes and save $1,083$ lives per year[1]. The Crash Avoidance Metrics Partnership (CAMP) is already working on creating common standards and a common technology for automakers to use so as they release fully functionall vehicles with V2V capability within the next 2 years.

Nevertheless, having the cars connected over an ad hoc network (VANET) does not come free of dangers; a compromisation of the car's security/defense system can give control to third parties over it. This is a feature that any 'computerized' car can suffer. Carjacking [3] events gradually appear in the news [4] and technical magazines [5]. While these incidents are currently limited, the availability in the near future of millions of vehicles with V2V capability raises the danger of 'epidemic' outbreaks over VANETs, where malicious software will infect large number of cars invalidating the benefits of V2V technology and even causing human casualties.

The study of epidemics has a long history in medicine and related areas [6], and has recenty seen a tremendous flourishing in the computer science realm [7] due to the great expansion of wired/wireless networks and portable devices and also due to the widespread use of online social networks (e.g., Facebook).

Among the issues pertaining to epidemics in computer networks, the topic of blocking the expansion of an epidemic has received significant attention reflecting the importance of protecting the unhindered operation of networks. However, the study of epidemic outbreak control so far has focused on: a) centralized methodologies where a network controller can make decisions over the network topology, b) on static or semi-static networks with no or very limited node mobility, and c) on the feasibility of the node or link removal operation which can take a node out of the network [8]. As far as existing VANET research on this topic is concerned, this has almost exclusively focused on modeling of the worm spreading process under various traffic conditions [9], [10], [11] and a scheme for patching the infected vehicles using cellular network's connectivity [11].

A. Motivation and contributions

Unfortunately, the aforementioned assumptions made by the existing works on epidemic control have little or no applicability at all in the VANET environment. A VANET is a highly distributed environment with opportunistic communication among vehicles, and clearly a fixed/centralized element (e.g., road-side unit) can not easily – due to cost and installation constraints – play the role of a detector and/or disinfector; even if a cellular network is provided for delivering patches, the density of infected vehicles in a region may prove to be a challenging environment for the base station to detect the malicious software and/or remove it. Moreover, the volatility of the network topology due to high vehicle mobility creates opportunities for effective blocking of the expansion (in case the infected vehicles are within an isolated component of a partitioned network) or make the blocking of it an extremely difficult task (in case that many infected vehicles are quickly

D. Katsaros' work was done while he was on sabbatical leave at Yale university.

[1]http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications

ISBN 978-3-901882-80-7 © 2016 IFIP

moving across all 'parts' of the network). Finally, it is not clear how could an infected vehicle be "thrown out" of the network, as it is done in static computer networks where part or all of the communication links of the infected computer are cut down or as it is done in human populations, where an infected individual may be quarantined; in VANETs, an infected vehicle may/can continue to transmit even if it is infected, continuing to spread the infection.

This article adopts a different perspective in the study of epidemics in the VANET environment by separating the task of infection blocking from the task of disinfection. The latter is highly dependent on the kind of software that creates the infection, on the particular type of vehicle that needs to be disinfected, and on the existence, coverage and capacity of wireless networks in the area of infection spreading; for instance the infected vehicle may need to be taken to a specialized car service point to be disinfected. On the contrary, the former task can be performed in-situ in a distributed fashion with the cooperation of other vehicles and minimal use of fixed infrastructure, and most importantly, techniques developed in the discipline of network science can be used for limiting the spreading of the epidemics. The present article proposes a cooperative technique which is the first one in the literature that utilizes V2V communications to "black-list" some (or potentially) infectious vehicles, and thus refrain other vehicles from accepting for processing packets transmitted by these vehicles. This technique can be seen as a node/link removal algorithm for blocking contagions appropriate for vehicular environments.

The present article makes the following contributions:

- It introduces the problem of blocking contagions in vehicular environments under the new perspective of separating the epidemic's blocking from the curing process.
- It introduces an epidemic blocking technique which is (almost) fully distributed making minimal use of fixed infrastructure to combat the expansion of the malicious software.
- It evaluates the proposed technique via simulations using established simulators to study its efficiency across a range of values of the most significant independent parameters that impact the performance of the method.

II. Related work

The present work is of relevance mainly to the topic of malware epidemics in VANETs and in complex networks in general, less related to the topic of security threats in VANETs, and remotely related to the defense methods for reliable vehicular communications. Worms can easily propagate through a network without any human intervention, and in recent years they have emerged as one of the most prominent threats to the security of computer networks [12], [13]. Effects of worm epidemics on VANETs have been recently studied in [9], [14], [11] and the common conclusion is that they pose a high level of danger; a worm attack on a VANET may interfere with critical applications such as engine control [15] and safety warning systems [3], hence resulting in serious congestion on the road networks and large-scale accidents.

There is an extensive body of literature on combating infections' expansion in complex networks based on node-removal methods [16], [17], based on link-removal methods [8], [18], [19]. Nevertheless, these works are not directly applicable in vehicular environemnts for the reasons explained in subsection I-A or because the proposed countermeasures [20], [21] do not fit a VANET.

In the area of security threats for VANETs, there are numerous kinds of attacks that may affect the reliable communication among the entities of a VANET such as Denial-of-Service (DoS) attack, fabrication attack, alteration attack, replay attack, message suppression attack, sybil attack [22]. Except from different kinds of attacks in terms of the used mechanism, there exist also other categories. For instance, a selfish driver could try to take advantage of the received information for personal benefit, while on the other hand a malicious attacker [23] aims to harm the users or the network with no profound personal gain.

A substantial amount of research on defense mechanisms has focused on intrusion detection systems for early detection of malicious nodes [24], [25], [26]. Regarding which, both specification-based [25] and anomaly-based treatments [26] have been investigated. Moreover, an attempt to deflect attacks using honeypots has been described in [27]. Finally, new techniques for filtering out tweaked data have been recently developed [28].

III. Virus Propagation

Spreading processes in complex networks is a widely studied topic that finds applications in varying disciplines [29]. Of particular importance is the problem of information propagation over complex networks, e.g., how information "travels" over networked populations such as Facebook. A well established and widely used model describing such processes is the *Susceptible-Infectious-Recovered* (SIR) model, borrowed from the literature of epidemiology. SIR models three possible states: Susceptible (**S**) state, where a node is vulnerable to infection, Infectious (**I**) state, where an infected node tries to infect its susceptible neighbors and succeeds with probability λ, and finally the Recovered (**R**) state, where a node has recovered (immunized) and can no longer get infected.

In correspondence, in vehicular networks a vehicle that can be affected by a virus will be a susceptible vehicle. Infectious vehicles will try to infected their current neighborhood, i.e., within transmission range, whereas recovered ones are either vehicles that cannot get infected (cf. V-D5) or those that have received a "cure", i.e., a patch that removes the virus and immunizes the vehicle in further contacts [11]. Unlike static networks, VANETS are characterized by a constantly changing topology due to transmission range limitations and obstacles or limited by geographic proximity and road topology. A vehicle becomes aware of its current neighboring vehicles through frequent exchange of beacon (*heartbeat*) messages and thus, the target set of an infectious source changes over time; from

sparse to dense neighborhoods and vice versa which evidently affects the diffusion dynamics.

Generally in wireless networks, nodes can communicate in a one-to-one fashion, i.e., *unicast*, one-to-some, i.e., *multicast* or one-to-all, i.e., *broadcast* communication. In a similar way we assume that a potential threat will follow one of the above mentioned methodologies to propagate to the next target(s). In our framework we focus on broadcast propagation. Finally one last characteristic that needs to be taken into consideration is the number of contacts, i.e., transmissions between I and S vehicles, needed for the virus to propagate. This final attribute will stand as a virus specific parameter regarding the strength of the virus, e.g., the length of the worm code or the way it is hidden within the exchanged messages. Hereafter we will refer to this attribute as the infection delay (τ) [11].

IV. Proposed Mechanism

A. Specialized Hardware (SH)

Since we have separated the functions of disinfecting from detecting infectious vehicles, we focus on the later and require a specialized hardware, namely SH, which will play the role of the detector and identify infected vehicles within its scanning range. We envision the SHs as stationary scanners and coordinators between the communicating vehicles rather than entrusting cars with that functionality. This is due to the fact that exploited security flaws that are severe enough to require physical interference to get rid of the infection, in occasions much like [30], can be more efficiently handled in a stationary SH. Thus, we conceive the SHs as highly secure devices initially deployed in a similar manner to Road Side Units (RSUs), that communicate and scan vehicles over the wireless medium.

In a wireless network when you have to keep the transmission power within acceptable limits, the overall efficiency of the network can be improved by either reducing the transmission rate or reducing the transmission range [31]. Based on this basic rule of thumb, and since the SHs must exchange high volumes of data with the vehicles that are under inspection, the transmission range of the SHs is kept low in order to be able to achieve high throughput. Only that way we can reassure that the vehicle can be fully scanned and correctly identified in terms of infection during its contact time with the SH.

B. Isolating Infectious Vehicles

Based on the fact that we can only detect malicious nodes as long as they are in the vicinity of an SH, it is not straightforward that the whole vehicular network can be protected. In the current work we assume that the SHs are only capable of identifying infected vehicles, but they are by no means capable of revoking the license of cars to participate in communication protocols [32]. Moreover, we expect that potential viruses attempting to spread over the network will be newfangled, i.e., there are no "predefined medicines" and thus a questionable amount of time may pass until an appropriate patch is ready for dispatching. Nonetheless, even if vehicles have some sort of access to a cellular service (e.g. 4G communication) enabling them to download and install a patch in sort time, there may be occasions where physical access to the car is necessary in order to carry out the hack, e.g., the Tesla case [30].

Thus our primary concern is to effectively mitigate the spreading of a virus in a vehicular network, until an appropriate patch arrives or "physical" treatment is administered. Although we may not be able to heal a vehicle or revoke its license, we are however capable of informing the rest of the vehicular network for its presence. Thus, SHs are also responsible for broadcasting the list of the so far identified infected vehicle ids, i.e., a *Black List* (BL). Hence, each healthy vehicle that "hears" the BL is instructed to shut all communication with those vehicles.

So far several considerations emerge. First, a vehicle that has not yet been in contact with an SH has no knowledge of the infected ids, and thus still stands unprotected against an (already identified) infected neighbor. Moreover, in each vehicle different versions of the BL may exist, depending on their last contact with an SH and the potentially newly identified infected vehicles in that interval. Thus the problem of outdated BLs arises. To this end vehicles are instructed to exchange their versions of the BL list, compare their own version with that of their neighbors, and hence cumulatively increase the awareness of their own and their near vicinity for the infected sources. This extension has a twofold benefit; first, isolated areas, i.e., areas relatively far from any SH may yet be protected, if an informed vehicle traverses the area. Since we will be able to deploy a limited number of SHs (due to infrastructure costs), vehicles must fill such "void spaces" by circulating the list. Second, the BL version of each vehicle is no longer based on the timestamp of its last contact with an SH, but is swiftly updated to the BL of the neighboring node with the most recent timestamp. Thus the possibility of significantly outdated BLs is minimized. Figure 1 is a simple illustration, where an infected vehicle A enters the range of the SH and infection is detected. Upon detection the SH broadcasts the list of all infected vehicles $-$currently only vehicle $A-$ which is heard from vehicle B and so on.

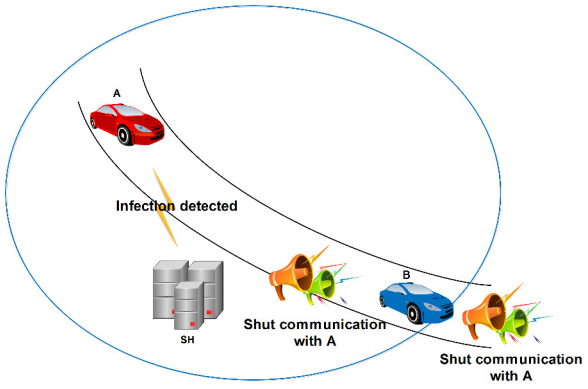

Fig. 1. Vehicle B is informed of A's infection by the SH. B will further broadcast (and exchange) its version of the BL with all other vehicles found in its trajectory.

Up to this point we detect and inform the vehicular network for the presence of infected vehicles, or in other words we *remove* nodes from the vehicular network. In correspondence, blocking epidemics in complex networks is a broadly addressed problem, where −among other techniques− researchers remove "important" nodes based on centrality measures, e.g. the degree centrality, to block the outspread of undesired propagations. It was found that removing the most connected nodes, the *hub* nodes, is a low cost and quite effective method. We cannot find complete equivalence in the different frameworks due to the very nature of $VANET$s, we can however exploit several points.

In [8] we proposed a method for blocking epidemics dynamically, i.e., during (and not prior to) the outbreak. Similarly, upon detecting an infectious vehicle the BL is updated and circulates within the network. So far through the proposed mechanism we diminish further damage that infected vehicles would exert in the system, if left undisturbed. Unfortunately we cannot estimate the time of infection of the identified vehicle, i.e., was the vehicle infected just a while ago or long before? In either case there is strong possibility that nearby vehicles (yet not scanned) are also infected. Hence maybe we can further protect the network by being cautious against the infected node's vicinity. To this end we maintain a second list, namely *Potentially Infected Vehicles* (PIV), where we include either all or a $fraction$ of an infected vehicle's current neighbors. Hereafter, we will refer to vehicles in BL as β, and respectively as π to those in the PIV list.

Similarly to the BL, PIV will be broadcasted from both vehicles and SHs. The difference between the two lists, is that vehicle ids in PIV are only temporarily banned from the system until those vehicles are scanned. Hence, once a π vehicle enters the range of an SH we have two possible outcomes. If the vehicle is found "clean", it is simply removed from PIV and its communication is restored. However if infection is detected, the vehicle is converted to β type (moved to BL) and all of its neighbors become π vehicles.

When the entire one hop neighborhood of a β is added in PIV the procedure is straightforward. However when only a fraction of those nodes is included, certain decision rules must be chosen that meet two basic criteria; fairness and efficiency. First, as we discussed earlier, removing highly connected nodes can be quite efficient in blocking the outspread of undesired propagations, or in other words those nodes can be very effective spreaders. Hence, choosing neighbors in decreasing order of their degree until the "cut", i.e., the desired fraction of neighborhood is attained and included in PIV, is our first intuition. Second, vehicles who had been in contact with a β car for a longer period, have a higher probability to be infected than more recent neighbors, especially for cases of large values of τ. Hence nodes are included in PIV in decreasing order of their contact duration, i.e., the oldest neighbor is included first and so forth.

A more sophisticated approach accounting for infected vehicles which meddle with the defense mechanism, i.e., meddle with either the BL or PIV or both, by broadcasting empty lists or meddle with the ids within is beyond the purpose of the current study and is left for future work. In this article, we try to protect the vehicular network from a potential virus spreading though vehicle nodes, by initiating another spreading process to counter its effect. This facet is formally known as: competing memes propagation on networks [33], where the meme, i.e., the virus or the list, which reaches/influences more nodes wins. Our intuitions lies in the belief that if we can inform a large number of nodes −through SH and vehicle (re)broadcasts− for infected and potentially infected nodes, we can significantly mitigate the spread of a worm-virus.

V. Experimental Design

A. Simulators

For the evaluation of our model, we use the simulator VEINS [34], which is composed of two well established and widely used simulators; OMNET++ an event-based network simulator and SUMO, a road traffic simulator.

B. Map

Integrated within VEINS, is the map of a City in Germany, namely *Erlangen*, which we used for our simulation. Figure 2 illustrates our experimented road topology. It is a rich road network environment of many intersections and different paths leading to various destinations. Note that the red boxes are buildings, i.e., obstacles interfering with the communication of vehicles. The locations of the SHs are also illustrated, however the optimal positioning for a set of n such computing devises is an open issue of many parameters. Setting aside budget constraints, i.e., number of available SH placements, we name just a few variables that we believe should be taken into consideration for an effective placement:

- the popularity of the road segments near an SH, i.e., frequently traversed road segments, namely *density driven* placement
- the number of routes passing through an area controlled by an SH, e.g., shortest paths, namely *topology driven* placement
- or social attributes such as city attractions, i.e., *social driven* placement

Nonetheless, investigating all such parameters individually (or in a combined scheme), is beyond the scope of the current study. In the current framework, we apply a simple allocation for the positions of the SHs by simply focusing in the center of the experimentation environment as illustrated in Figure 2. Note that buildings will interfere in both the transmission range of vehicles and the scanning process of the SHs.

C. Initially Infected Vehicles

As illustrated in [11], a single vehicle is enough to contaminate the entire network. Following the same policy, we initiate the malware propagation from a single spreader. However, our experimentation showed that initiating the infection from different positions yields different results. This is due to the fact that the different vehicles will experience different conditions, i.e., different number of neighboring vehicles, different speeds

Fig. 2. Part of the Erlangen city. SHs are positioned near the center of the map. The illustrated scanning region is indicative, to highlight the relatively short range of the specialized hardware devices.

and directions between them, etc. Furthermore the relative position of the initial spreader and the relative position of the SHs also plays a crucial role for the spreading dynamics of the virus. For instance, if the initial spreader falls within the range of an SH in short time after it starts its malicious behavior, the spreading process is very likely to stop very quickly, especially for the larger values of τ. In our experimentation we avoid such cases.

With the above consideration we experimented with a wealth of different positions for the initially infected vehicle as illustrated with the different points in Figure 2, e.g., A, X, etc. The infection starts after running the simulation for 100 seconds whereas the total simulation time is 500 seconds. For each point the results were averaged over ten distinct runs.

D. Vehicle Settings

1) Communication: We assume that all cars are capable of communicating with $DSRC$; according to [35] an acceptable communication range for vehicle applications is about $300m$ and this is used in our simulation. This range that can be achieved by low transmission power is enough for correct dissemination of a message in a neighborhood while it improves spatial reuse in heavy traffic. In rural environments, in scenarios with low data rate (3Mbps) authors in [35] showed that Packet Delivery Ratio (PDR) of 60% can be achieved for such medium distances.

2) Routes & Density: For selecting the trajectories that vehicles will follow in our simulation, we applied the predefined tools within the road traffic simulator SUMO to obtain a diverse range of routes. Specifically a total of 30 different routes were produced. The density of the vehicle nodes is measured in per hour basis. Specifically we experimented with values of 1000 to 2500 with a step of 500, to imprint light and heavy traffic simulations, i.e., a sparse or dense vehicular network.

3) Velocity: For the speed of vehicles and with regard to an uban environment's restrictions, we draw a uniform distribution between 8-$14m/s$ for each car that enters the simulation. Hence each respective vehicle has its own desired speed, which coupled with the different density values, generates a highly dynamic environment.

4) Neighborhood: The neighbor list for each vehicle is maintained by the periodic exchange of beacon messages. A typical beacon includes information about a vehicle's id, its position and speed. In our experimentation beacons are broadcasted every one second. To account for cases where messages are temporarily lost, e.g. due to building-obstacles, and not due to a car getting out of range, a vehicle removes a neighbor if it missed two consecutive beacon messages.

5) Virus Strength: Lastly, it is reasonable to assume that a virus may not be able to "penetrate the defenses" of all vehicles it encounters [11]. This may be due to manufacturing aspects, antivirus flaws, etc. Thus, the virus is characterized by a final parameter, namely the *Virus Strength (VS)* indicating the number of vehicles in the simulation that are vulnerable to it. Hence, vehicles that cannot get infected, are set in the R state of the SIR spreading model, i.e., immune vehicles.

VI. Results

Summarized in Table I are the experimentation parameters used in our simulation. Unless stated otherwise default values are used. Evidently when SHs have a broader scanning range, more vehicles are identified through the specialized hardware. In order to highlight the fact that the proposed method is efficient due to the dissemination of the lists (BL, PIV) among vehicles we keep the scanning range of the SHs to $30m$ for the entire simulation. Moreover, unlike static networks where the number of deletions is limited [8] [36], in a VANET nodes can be deleted in a broadcast fashion. Hence we choose to cut either all or half of the neighborhood of an infected source as explained in subsection IV-B. Overall, the illustrated results are a fraction of the experimentation we conducted. In the current article we illustrate the most characteristic ones, nonetheless the qualitative conclusions are the same.

TABLE I
Simulation Parameters

Parameters	Range	Default
Infection Delay (τ)	1 - 6	4
Vehicle Speed (m/s)	8 - 14	Uniform
Vehicle Density (per Hour)	1000 - 2500	1500
SH Scan Range (m)	30	30
Cut (%)	50 - 100	100
Vehicle Transmission Range (m)	300	300
Virus Strength (%)	25 - 100	100

A. Impact of Vehicle Density & Different Initial Spreader

In this first subsection we evaluate the performance of the proposed technique as we increase in density, i.e., the

number of vehicles. The results are illustrated in Figures 3 (by infection point) and 4 (by averages). When diffusion processes are in progress, higher density means more available paths for the spreading. This attribute will increase the difficulty for any defense mechanism to block the outspread of the infection. However, in our framework, this situation enhances the spreading of the virus negating elements, i.e., the BL and PIV lists, hence increases the efficiency of the proposed method.

By observing the results in Figure 3 we understand that different starting points of the initial infected vehicle can yield different results. This is due to the fact that vehicles experience different local environments; different number of one hop neighbors ranging from only a few to dozens; neighbors who co-travel for a long period or only for a few seconds; different speeds and directions between them etc. It is worth noting that the map (Figure 2) used in our simulation has a wealth of obstacles (buildings) which interfere with the communication of vehicles. Moreover there are several locations which favor the spreading process more than others. For example, Area 1 mostly allows spreading in a vertical or horizontal fashion. In Area 2 horizontal transmissions are often blocked. On the other hand in Area 3 or around the area of $SH1$, transmissions occur in all possible directions (horizontal, vertical, diagonal, etc.) due to the existence of large open areas, i.e., sparser buildings locations, providing a more favorable environ for the virus to propagate faster with respect to the other areas. Hence, it can be concluded that these network parameters, play significant role in the spreading of the virus and the diffusion dynamics of our defense mechanism. This is partially the reason for the diversity of the results in terms of the percentage of the infected network as illustrated in Figure 3. By further analyzing Figure 3 we can classify the initial infectors into three groups; *increasing*, i.e., as we increase in density the infection worsens, such as vehicles of points E or Z; relatively *steady* (or non-epidemic) as points C, D or F; and finally *spiked* as points A, G or Y, i.e., infectors whose behavior is highly depended on the network parameters as previously discussed.

Examining Figure 4, we observe that when we have a sparse network and include 100% of an infected vehicle's vicinity in our PIV list, the infection is non-epidemic, i.e., only about 10% of the vehicles get infected. Reminisce that the infection delay is four tranmsissions ($\tau = 4$). As vehicle density increases from 1000 V/h to 1500 V/h, the average percentage of the network that is infected also increases. For values between 1500 V/h and 2000 V/h the percentage remains steady, although in real numbers there is a linear dependence between density and infected vehicles. For values above 2000 V/h the percentage of infected vehicles starts to decrease. This is partially due to the fact that with increased density more neighbors are included in PIV and thus the dissemination paths of the virus are significantly reduced. On the other hand for the proposed mechanism those paths are only increasing, which coupled with the fact that only a single transmission is needed to circulate the PIV and BL lists (in contrast to $\tau = 4$ for the spread of the virus) enhances the effectiveness of the mechanism.

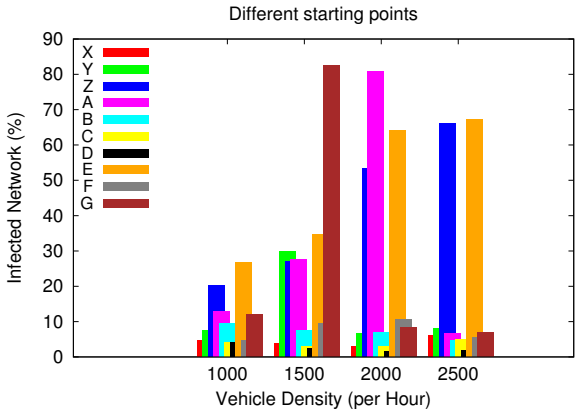

Fig. 3. Percentage of the infected network from the different initial spreading points.

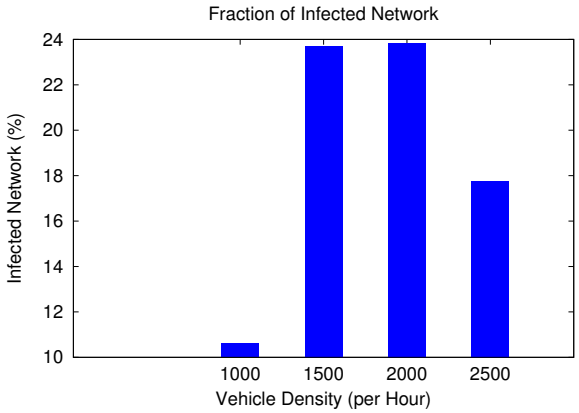

Fig. 4. Average infected network size.

B. Impact of Infection Delay (τ)

Next we investigate on the impact of the infection delay (τ). Evidently increasing the number of necessary transmissions for the virus to propagate has a positive impact on the proposed defense method. In other words, the longer it takes for the virus to travel from vehicle-to-vehicle, the more time we gain to circulate both, the PIV and BL lists within the vehicular network. Moreover the existence of obstacles will further delay the propagation of the virus, whereas the proposed technique will be less influenced since a single transmission is needed to inform susceptible vehicles. As illustrated in Figure 5, when $\tau = 1$, meaning that the infection is instantaneous between vehicles, the infection is near 80% (i.e., most of the network gets infected) since the defense mechanism cannot propagate faster than the dissemination of the virus. In this extreme occasion any similar defense mechanism would prove inadequate to block the outspread of the virus. For $\tau = 2$ the diffusion of the virus is significantly mitigated through the

proposed technique, whereas for $\tau = 6$ the infection is limited to only 10% of the vehicular network.

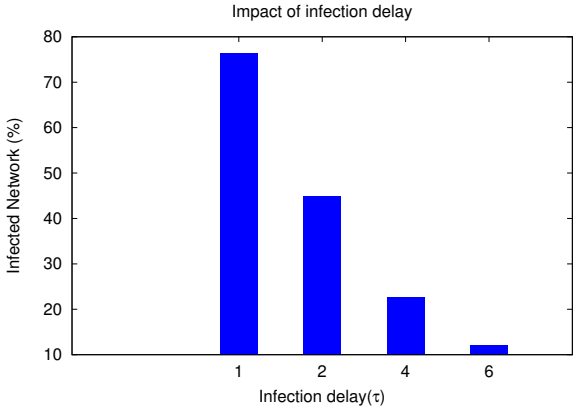

Fig. 5. Impact of the tranmissibilty of the virus.

C. Impact of Virus Strength

In Figure 6 the x-axis represents the fraction of the network nodes susceptible to infection. The results illustrate that when the number of vehicles that are vulnerable to infection decrease, then the spreading of the virus also decreases. This is due to the fact that the network from the perspective of the virus, becomes more sparse than it really is and potentially disconnected. On the other hand, this feature only affects positively the proposed method, since these "firewall" nodes will hinder only the spread of the virus while the circulation of PIV and BL is left undisturbed.

Since the spreading paths for the virus are gradually diminishing, the virus "speed" is mostly based on the respective vehicle's velocity and the topological characteristics of the road network in order to overcome the potential disconnected paths. Under these circumstances, the ability of the virus to become epidemic is questionable. On the other hand, even when 100% of the network is vulnerable to infection, only about 23% of the VANET is infected which highlights the efficiency of the proposed mechanism.

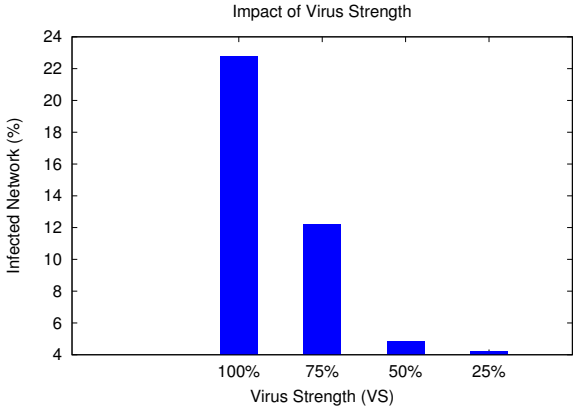

Fig. 6. Vulnerability of vehicles to infection.

D. Impact of Different Cut Methods

By decreasing the percentage of the neighbors of an infected node that are blocked (included in PIV), we expect that the efficiency of the proposed technique will also decrease. Thus the question at hand is which is the better criterion to choose, i.e., cut nodes based on their connectivity (degree) or their contact duration. Figure 7 illustrates that cutting nodes based on the largest degree yields better results. This is due to the fact that in an urban environment we cannot expect the flow of vehicles to be smooth. For instance, the existence of upcoming congested intersections, roads of different priorities or road segments occupied by a large number of vehicles, will result in a disturbed traffic environment causing vehicles to slow down or line up for arbitrary lengths of time. Thus, in such cases choosing nodes with respect to contact duration will be less efficient. On the other hand, by selecting vehicles in decreasing order of connectivity, i.e., locally more central nodes, the proposed mechanism is found more efficient in blocking the outspread of the virus.

The last subject to discuss concerns vehicles which are included in PIV, but are not truly infected. For instance when applying the degree cut method with default settings and initiate the infection from point X, we observed that out of 153 vehicles included in PIV, 30 vehicles where not truly infected. Although this is not a negligible portion of vehicle nodes, our results indicate that a more sophisticated cut method can reduce those "false positives" even more. Overall, moving vehicles in PIV means cutting communication paths for vehicles that may not be infected, which can result in additional delay and hinder Quality of Service (QoS) for applications running on VANETS. Nonetheless this is only a temporal (but necessary) effect of the proposed technique, for efficiently blocking the outspread of the virus.

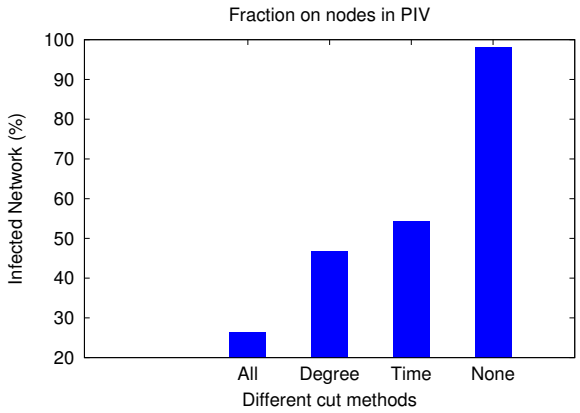

Fig. 7. Cutting different neighbors from infected nodes.

VII. Conclusion

In the current article we proposed a distributed algorithm for hindering the outspread of a virus in vehicular networks. By circulating −among the vehicles− the list of the ids of the currently identified infected nodes and a set of their neighborhood, we try to shield the remaining network from the infected

sources and ”outrun” the virus. Our simulation showed that the proposed mechanism significantly hindered the outspread of the virus even when the entire network was susceptible to infection. An interesting direction resides in devising more sophisticated approaches towards a better selection from the infectors vicinity, e.g., by applying different cuts with respect to local network parameters. Finally, a challenging task that remains, is the enhancement of the proposed mechanism to defend against “smarter” viruses capable of hiding from any similar detection mechanism, e.g., by the use of multiple pseudonyms. As the proposed method stands, its performance will vary with respect to the flexibility of the virus to change a vehicle’s id.

Acknowledgments: D. Katsaros has been co-financed by the EU (European Social Fund - ESF) and Greek national funds through the Operational Program “Education and Lifelong Learning” of the National Strategic Reference Framework (NSRF) - Research Funding Program: Thales - Investing in knowledge society through the European Social Fund in the context of the project “Social network aware cognitive radio networks – SoCoNet (no. 85459)”.

REFERENCES

[1] S. Joerer, M. Segata, B. Bloessl, R. Lo Cigno, C. Sommer, and F. Dressler, “A vehicular networking perspective on estimating vehicle collision probability at intersections,” *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 4, pp. 1802–1812, 2014.

[2] D. Caveney, “Cooperative vehicular safety applications,” *IEEE Control Systems magazine*, vol. 30, no. 4, 2010.

[3] J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[4] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[5] W. Knight, “Rebooting the automobile,” *MIT Technology Review*, vol. 118, no. 4, pp. 54–59, 2015.

[6] R. M. Anderson and R. M. May, *Infectious Diseases of Humans: Dynamics and Control*. Oxford University Press, 1992.

[7] C. Nowzari, V. M. Preciado, and G. J. Pappas, “Analysis and control of epidemics: A survey of spreading processes on complex network,” tech. rep., 2015. Available at: http://arxiv.org/abs/1505.00768.

[8] P. Basaras, D. Katsaros, and L. Tassiulas, “Dynamically blocking contagions in complex networks by cutting vital connections,” in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1170–1175, 2015.

[9] L. Cheng and R. Shakya, “VANET worm spreading from traffic modeling,” in *Proceedings of the IEEE Radio and Wireless Symposium (RWS)*, pp. 669–672, 2010.

[10] M. Nekovee, “Modeling the spread of worm epidemics in vehicular ad hoc networks,” in *Proceedings of the IEEE Vehicular Technology Conference-Spring (VTC-Spring)*, pp. 841–845, 2006.

[11] O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, “Understanding, modeling and taming mobile malware epidemics in a large-scale vehicular network,” in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM)*, 2013.

[12] T. M. Chen and J.-M. Robert, “Worm epidemics in high-speed networks,” *IEEE Computer magazine*, vol. 37, no. 6, pp. 48–53, 2004.

[13] E. Mojahedi and M. A. Azgomi, “Modeling the propagation of topology-aware p2p worms considering temporal parameters,” *Peer-to-Peer Networking and Applications*, vol. 8, no. 1, pp. 171–180, 2015.

[14] S. A. Khayam and H. Radha, “Analyzing the spread of active worms over VANET,” in *Proceedings of the ACM International Workshop on Vehicular Ad hoc Networks (VANET)*, pp. 86–87, 2004.

[15] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental security analysis of a modern automobile,” in *Proceedings of the IEEE Symposium in Security and Privacy (SP)*, pp. 447–462, 2010.

[16] L. Hebert-Dufresne, A. Allard, J. G. Young, and L. J. Dube, “Global efficiency of local immunization on complex networks,” *Nature Scientific Reports*, vol. 3, 2013.

[17] C. J. Kuhlman, G. Tuli, S. Swarup, M. V. Marathe, and S. S. Ravi, “Inhibiting diffusion of complex contagions in social networks: Theoretical and experimental results,” *Data Mining and Knowledge Discovery*, vol. 29, no. 2, pp. 423–465, 2015.

[18] M. Kimura, K. Saito, and H. Motoda, “Minimizing the spread of contamination by blocking links in a network,” in *Proceedings of the National Conference on Artificial Intelligence (AAAI)*, vol. 2, pp. 1175–1180, 2008.

[19] C. J. Kuhlman, G. Tuli, S. Swarup, M. V. Marathe, and S. S. Ravi, “Blocking simple and complex contagion by edge removal,” in *Proceedings of the IEEE International Conference on Data Mining (ICDM)*, pp. 399–408, 2013.

[20] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, “Defending against hitlist worms using network address space randomization,” *Computer Networks*, vol. 51, no. 12, pp. 3471–3490, 2007.

[21] L. Fan, Z. Lu, W. Wu, B. Thuraisingham, H. Ma, and B. Y., “Least cost rumor blocking in social networks,” in *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp. 540–549, 2013.

[22] J. R. Douceur, “The sybil attack,” in *Proceedings of the International Workshop on Peer-to-Peer Systems (IPTPS)*, pp. 251–206, 2002.

[23] L. Buttyan, T. Holczer, and I. Vajda, “On the effectiveness of changing pseudonyms to provide location privacy in VANETs,” in *Security and Privacy in Ad-hoc and Sensor Networks*, vol. 4572 of *Lecture Notes in Computer Science*, pp. 129–141, 2007.

[24] L. A. Maglaras, “A novel distributed intrusion detection system for vehicular ad hoc networks,” *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 4, pp. 101–106, 2015.

[25] U. E. Larson, D. K. Nilsson, and E. Jonsson, “An approach to specification-based attack detection for in-vehicle networks,” in *Proceedings of the IEEE Intelligent Vehicles Symposium*, pp. 220–225, 2008.

[26] M. Muter, A. Groll, and F. C. Freiling, “A structured approach to anomaly detection for in-vehicle networks,” in *Proceedings of the IEEE International Conference on Information Assurance and Security (IAS)*, pp. 92–98, 2010.

[27] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, “An approach to using honeypots in in-vehicle networks,” in *Proceedings of the IEEE Vehicular Technology Conference-Fall (VTC-Fall)*, 2008.

[28] P. Basaras, L. A. Maglaras, D. Katsaros, and H. Janicke, “A robust eco-routing protocol against malicious data in vehicular network,” in *Proceedings of the IFIP Wireless and Mobile Networking Conference (WMNC)*, 2015.

[29] B. H. Javier, R. A. Banos, B. S. Gonzalez, and Y. Moreno, “Cascading behaviour in complex socio-technical networks,” *Journal of Complex Networks*, vol. 1, pp. 3–24, 2013.

[30] http://www.computerworld.com/article/2960802/security/tesla-patches-model-s-after-researchers-hack-cars-software.html.

[31] J. Guo and N. Balon, “Vehicular ad hoc networks and dedicated short-range communication,” *Univesity of Michigan, September*, vol. 22, 2006.

[32] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of misbehaving and faulty nodes in vehicular networks,” *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1557–1568, 2007.

[33] X. Wei, N. Valler, B. Prakash, I. Neamtiu, M. Faloutsos, and C. Faloutsos, “Competing memes propagation on networks: A network science perspective,” *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 6, pp. 1049–1060, 2013.

[34] C. Sommer, R. German, and F. Dressler, “Bidirectionally coupled network and road traffic simulation for improved IVC analysis,” *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, 2011.

[35] F. Bai, D. Stancil, and H. Krishnan, “Toward understanding characteristics of Dedicated Short Range Communications (DSRC) from a perspective of vehicular network engineers,” in *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, pp. 329–340, 2010.

[36] H. Tong, B. A. Prakash, T. Eliassi-Rad, M. Faloutsos, and C. Faloutsos, “Gelling, and melting, large graphs by edge manipulation,” in *Proceedings of the ACM International Conference on Information and Knowledge Management (CIKM)*, pp. 245–254, 2012.