NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCE
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

POSTGRADUATE PROGRAM

THESIS

Vulnerability of parking assistance systems to vehicular node misbehaviors

Georgios K. Kollias
Maria G. Papadaki

Supervisors: **Ioannis Stavrakakis,** Professor
Merkouris Karaliopoulos, Research Associate

ATHENS

JANUARY 2013

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη της ανθεκτικότητας των συστημάτων υποβοήθησης στάθμευσης σε κακόβουλες συμπεριφορές οχημάτων

Γεώργιος Κ. Κόλλιας
Μαρία Γ. Παπαδάκη

Επιβλέποντες: **Ιωάννης Σταυρακάκης,** Καθηγητής
Μερκούρης Καραλιόπουλος, Επιστημονικός Συνεργάτης

ΑΘΗΝΑ

ΙΑΝΟΥΑΡΙΟΣ 2013

THESIS

Vulnerability of parking assistance systems to vehicular node misbehaviors

Georgios K. Kollias

R.N.: M1153

Maria G. Papadaki

R.N.: M1140

SUPERVISORS: **Ioannis Stavrakakis,** Professor
Merkouris Karaliopoulos, Research Associate

ADVISORY COMMITTEE: **Athanasia Alonistioti,** Lecturer

January 2013

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη της ανθεκτικότητας των συστημάτων υποβοήθησης στάθμευσης σε κακόβουλες συμπεριφορές οχημάτων

Γεώργιος Κ. Κόλλιας

Α.Μ.: Μ1153

Μαρία Γ. Παπαδάκη

Α.Μ.: Μ1140

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Ιωάννης Σταυρακάκης,** Καθηγητής
Μερκούρης Καραλιόπουλος, Επιστημονικός Συνεργάτης

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: **Αθανασία Αλωνιστιώτη,** Λέκτορας

Ιανουάριος 2013

ABSTRACT

In competitive networking environments, user nodes try to serve their own interests, taking as much as possible advantage of the available information and having the option to either cooperate or compete with other user nodes. In this paper we investigate a real-world scenario of parking assistance service that instantiates such environments. Under the nominal-altruistic operation, the vehicles opportunistically collect and share information on the location and availability status of each parking spot they encounter as they drive around. Yet the competition for parking spots may give rise to various facets of misbehaviors. The two intuitive instances we analyze involve drivers deferring from sharing their information (*free-riders*) and deliberate falsifying disseminated information so as to divert other drivers away from a particular area of own interest (*selfish liars*). The simulation results indicate a persistent *fate-sharing* effect; namely the misbehaving nodes fail to obtain any substantial performance advantage over what the cooperative nodes achieve. On the contrary, misbehaviors, when of adequate intensity, tend to reduce the destination-occupied spot distance for *all* vehicles at the expense of higher parking search times, which quickly become prohibitive when the vehicles' destinations overlap. Mobile storage nodes (*bona fide mules*) compensate the reduction of the information flow due to free-riders but, as also shown with mean-field theoretic arguments, have almost no effect against selfish liars since they end up propagating the falsified information those nodes generate. Finally, we take into consideration the case where misbehaving nodes in a centrally assisted parking search system try to bypass sometimes system's procedure, when destinations are uniformly distributed, in order to obtain a better spot than the one the assigned to them. Results show that these *position stealers* cannot harm the system performance.

SUBJECT AREA: Vehicular networks

KEYWORDS: parking assistance systems, non-cooperative opportunistic dissemination

ΠΕΡΙΛΗΨΗ

Στα ανταγωνιστικά δικτυακά περιβάλλοντα, οι κόμβοι προσπαθούν να εξυπηρετήσουν τα δικά τους συμφέροντα, χρησιμοποιώντας όσο περισσότερο μπορούν προς όφελος τους τη διαθέσιμη πληροφορία και έχοντας ως επιλογή είτε να συνεργαστούν με άλλους κόμβους, είτε να τους ανταγωνιστούν. Σε αυτή την εργασία μελετάμε ένα ρεαλιστικό σενάριο υπηρεσίας υποβοήθησης στάθμευσης που μοντελοποιεί αυτά τα περιβάλλοντα. Σύμφωνα με την ιδανική-αλτρουϊστική λειτουργία, τα οχήματα συλλέγουν και διαμοιράζουν μεταξύ τους πληροφορίες σχετικές με την τοποθεσία και την διαθεσιμότητα κάθε θέσης στάθμευσης που συναντούν καθώς κινούνται. Όμως ο ανταγωνισμός για τις θέσεις στάθμευσης μπορεί να δώσει αφορμή για την εκδήλωση κακόβουλων συμπεριφορών. Οι δύο περίπτωσεις που αναλύουμε περιλαμβάνουν οδηγούς που δεν συμμετέχουν στον διαμοιρασμό της πληροφορίας τους με τους άλλους οδηγούς (free-riders) και που εσκεμμένα διαδίδουν λανθασμένες πληροφορίες για να απομακρύνουν τους άλλους οδηγούς από την περιοχή ενδιαφέροντός τους (selfish liars). Τα αποτελέσματα της προσομοίωσης δείχνουν μία επίμονη fate-sharing επίδραση: συγκεκριμένα οι κόμβοι που δρουν κακόβουλα αδυνατούν να αποκτήσουν κάποιο ουσιώδες πλεονέκτημα σε σύγκριση με αυτό που επιτυγχάνουν οι συνεργάσιμοι κόμβοι. Αντίθετα, οι κακόβουλες συμπεριφορές, όταν εκδηλώνονται με επαρκή ένταση, τείνουν να μειώσουν την απόσταση προορισμού-δεσμευμένης θέσης για όλα τα οχήματα ξοδεύοντας περισσότερο χρόνο αναζήτησης, ο οποίος γίνεται σύντομα απαγορευτικός όταν οι προορισμοί των οχημάτων επικαλύπτονται. Οι κινητοί κόμβοι αποθήκευσης (bona fide mules) αντισταθμίζουν την επίδραση των free-riders, αλλά όπως φαίνεται μέσω θεωρητικών συλλογισμών, δεν έχουν σχεδόν καμία επίδραση απέναντι στους selfish liars καθώς καταλήγουν να διαδίδουν τις λανθασμένες πληροφορίες που οι τελευταίοι παράγουν. Τελειώνοντας, λαμβάνουμε υπόψιν μας την περίπτωση όπου οι κακόβουλοι κόμβοι σε ένα κεντρικοποιημένο σύστημα υποβοήθησης στάθμευσης, προσπαθούν να παρακάμψουν την διαδικασία που ακολουθεί το σύστημα, όταν οι προορισμοί είναι ομοιόμορφα κατανεμημένοι, για να δεσμεύσουν καλύτερη θέση από εκείνη που τους έχει ανατεθεί. Τα αποτελέσματα από την μελέτη αυτής της περίπτωσης δείχνουν ότι οι position stealers δεν μπορούν να επηρρεάσουν την απόδοση του συστήματος.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Δίκτυα οχημάτων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: συστήματα υποβοήθησης στάθμευσης, μη-συνεργατική οπορτουνιστική διάδοση

ACKNOWLEDGEMENTS

We would like to express our kindest greetings to the Ph.D. student, Ms. Evangelia Kokolaki and Research Associate, Dr. Merkouris Karaliopoulos for the excellent cooperation we have had during the last year in order to reach this important milestone. It's a pleasure for us to work with people like Evangelia and Merkouris and we would like to wish them the best for both their careers and personal lives.

Furthermore, we would like to thank our supervisor Professor Ioannis Stavrakakis for providing us the means and the support to prepare and deliver this work.

This work has been supported in part by the European Commission through the ICT FET project RECOGNITION (FP7-IST-257756) , the Network of Excellence in Internet Science project EINS (FP7- IST- 288021) and the Marie Curie grant RETUNE (FP7-PEOPLE-2009-IEF- 255409).

ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ

Σε αυτή την εργασία εξετάζουμε εκτεταμένα την ανθεκτικότητα των οπορτουνιστικών συστημάτων υποβοήθησης στάθμευσης όταν η συμπεριφορά των οδηγών χαρακτηρίζεται από ελλιπή συνεργασία. Σύμφωνα με την ιδανική-αλτρουιστική λειτουργία, τα οχήματα συλλέγουν και διαμοιράζουν μεταξύ τους πληροφορίες σχετικές με την τοποθεσία και την διαθεσιμότητα κάθε θέσης στάθμευσης που συναντούν καθώς κινούνται. Όμως ο ανταγωνισμός για τις θέσεις στάθμευσης μπορεί να δώσει αφορμή για την εκδήλωση κακόβουλων συμπεριφορών, με άμεσες συνέπειες στο μέσο χρόνο αναζήτησης στάθμευσης καθώς και στην απόσταση μεταξύ των τελικών θέσεων στις οποίες οι οδηγοί καταλήγουν και των πραγματικών προορισμών τους. Το διπλό ερώτημα που προκύπτει από την πλευρά των οδηγών είναι εάν οι κόμβοι έχουν κίνητρα να δράσουν κακόβουλα και κατά πόσο αυτή η δράση τους επιτρέπει να επιτύχουν καλύτερους χρόνους αναζήτησης και/ή αποστάσεις θέσης-προορισμού.

Οι δύο περιπτώσεις κακόβουλης συμπεριφοράς που αναλύουμε περιλαμβάνουν οδηγούς που δεν συμμετέχουν στον διαμοιρασμό της πληροφορίας τους με τους άλλους οδηγούς (free-riders) και που εσκεμμένα διαδίδουν λανθασμένες πληροφορίες για να απομακρύνουν τους άλλους οδηγούς από την περιοχή ενδιαφέροντός τους (selfish liars). Προσομοιώνουμε έναν μεγάλο αριθμό κρίσιμων παραμέτρων κάτω από διαφορετική ένταση κακόβουλης συμπεριφοράς, όταν οι προορισμοί των οχημάτων είναι ομοιόμορφα κατανεμημένοι και όταν επικαλύπτονται. Επιπρόσθετα, μελετάμε το αποτέλεσμα της εισαγωγής κινητών κόμβων αποθήκευσης (mobile relay nodes - MSNs) στην προσπάθεια μας να αντισταθμίσουμε την επίδραση των κακόβουλων συμπεριφορών στο σύστημα όταν οι προορισμοί επικαλύπτονται. Τέλος, πραγματοποιούμε μία συνοπτική μελέτη της επίδρασης που μπορεί να έχει η παρουσία κακόβουλων κόμβων σε ένα κεντρικοποιημένο σύστημα υποβοήθησης στάθμευσης όπου οι προορισμοί είναι ομοιόμορφα κατανεμημένοι. Συγκεκριμένα, η περίπτωση που εξετάζουμε σχετίζεται με κόμβους που δεν βασίζονται αποκλειστικά στη καθοδήγηση του συστήματος για την εύρεση ελεύθερης θέσης στάθμευσης (position stealers), όπως συμβαίνει στην ιδανική λειτουργία των συστημάτων αυτών.

Η υπο μελέτη εξέταση πραγματοποιείται μέσα σε ένα πολυπαραμετρικό, δυναμικό περιβάλλον με χαρακτηριστικά που αλλάζουν στο χώρο και το χρόνο· κάτι που δεν ευνοεί τη θεωρητική προσέγγιση του προβλήματος. Συνεπώς, η μελέτη πραγματοποιείται μέσω προσομοιώσεων, ενώ η μοντελοποίηση χρησιμοποιείται περιστασιακά για την θεωρητική υποστήριξη των πορισμάτων της προσομοίωσης. Τα αποτελέσματα που προκύπτουν δεν είναι σε όλες τις περιπτώσεις διαισθητικά αναμενόμενα. Συγκεκριμένα σε ένα οπορτουνιστικό σύστημα υποβοήθησης στάθμευσης, οι κόμβοι που δρουν κακόβουλα αδυνατούν να αποκτήσουν κάποιο ουσιώδες πλεονέκτημα σε σύγκριση με αυτό που επιτυγχάνουν οι συνεργάσιμοι κόμβοι. Παρ' όλα αυτά, οι δύο τύποι κακόβουλων συμπεριφορών τείνουν, σχεδόν σε όλες τις περιπτώσεις, να μειώσουν τις αποστάσεις θέσης-προορισμού και να αυξήσουν το χρόνο αναζήτησης για όλα τα οχήματα, με την τελευταία αύξηση να γίνεται ιδιαίτερα έντονη όταν οι προορισμοί των οδηγών επικαλύπτονται. Αντίθετα, καμία από τις δύο συμπεριφορές δεν περιορίζει τα φαινόμενα συγχρονισμού που εμφανίζονται στα περιεχόμενα της μνήμης, λόγω της οπορτουνιστικής ανταλλαγής περιεχομένων. Κατά συνέπεια, τα μοτίβα κίνησης/οι διαδρομές των οχημάτων παραμένουν σε ένα μεγάλο βαθμό κοινές, ιδιαίτερα όταν οι προορισμοί τους επικαλύπτονται. Η εισαγωγή των MSNs λειτουργεί ως αποτελεσματικό αντίμετρο στην περίπτωση αυτή όταν οι κόμβοι συμπεριφέρονται ως free-riders, ενώ βοηθούν ελάχιστα όταν οι κόμβοι είναι selfish liars. Όσον αφορά το κεντρικοποιημένο σύστημα, η εκδήλωση της κακόβουλης συμπεριφοράς που εξετάζεται δε φαίνεται να έχει καμία επίδραση στην απόδοση του συστήματος, επιβεβαιώνοντας τις καλύτερες επιδόσεις του σε θέματα ανθεκτικότητας.

CONTENTS

1. INTRODUCTION 16

2. OPPORTUNISTICALLY ASSISTED PARKING SEARCH AND IMPERFECT COOPERATION 18

3. PERFORMANCE EVALUATION METHODOLOGY 20

3.1 Simulation Environment 20

3.2 Simulation set-up and performance metrics 21

4. SIMULATION RESULTS - EXPERIMENTATION 22

4.1 Uniformly distributed travel destinations 22

4.1.1 Information Denial 22

4.1.2 Information Forgery 24

4.2 Hotspot Scenario 26

4.2.1 Information Denial 26

4.2.2 Information Forgery 27

4.3 Mobile Storage Nodes for the hotspot scenario 28

4.3.1 Information Denial 29

4.3.2 Information Forgery 29

4.4 Centrally assisted parking search 31

5. RELATED WORK 33

6. CONCLUSION 34

ACRONYMS 35

ANNEX I 36

REFERENCES 40

LIST OF FIGURES

Figure 1: Average parking search time..23

Figure 2: Average destination-spot distance..23

Figure 3: Average distance from destination of spot records at vehicles' caches..........23

Figure 4: Ratio of parking attempts in RM mode 23

Figure 5: Ratio of parking attempts in FM mode...23

Figure 6: Ratio of successful parking attempts in FM mode 24

Figure 7: Ratio of successful parking attempts in FM mode over all successful attempts 24

Figure 8: Average parking search time..25

Figure 9: Average destination-spot distance..25

Figure 10: Ratio of parking attempts in FM mode...25

Figure 11: Average parking search time..25

Figure 12 Average destination-spot distance:..25

Figure 13: Ratio of parking attempts in FM mode...26

Figure 14: Average parking search time..27

Figure 15: Average destination-spot distance..27

Figure 16: Average number of records in memory 27

Figure 17: Average parking search time..28

Figure 18: Average destination-spot distance..28

Figure 19: Average number of records in memory 28

Figure 20: Average parking search time..29

Figure 21: Average destination-spot distance..29

Figure 22: Average parking search time..31

Figure 23: Average destination-spot distance..31

Figure 24: Average parking search time..32

Figure 25: Average destination-spot distance..32

Figure 26: Number of parked vehicles 32

LIST OF PICTURES

Picture 1: VANETs' applications 36

LIST OF TABLES

Table 1: Simulation parameters..21

Table 2: Misbehaving nodes' profiles 38

PREFACE

The research described in this MCs thesis was conducted by M.Sc. students George K. Kollias and Maria G. Papadaki, with the contribution of the Ph.D. student Evangelia Kokolaki. It was undertaken within the MCs program “Communication Systems and Networks”, in the department of Informatics and Telecommunications, National and Kapodistrian University of Athens during the period November 2011 – January 2013. The supervisors of this thesis were Prof. Ioannis Stavrakakis and Research Associate Merkouris Karaliopoulos.

1. INTRODUCTION

In various mobile applications involving competition for scarce resources, networked entities (user nodes) have to autonomously decide whether to dispose private information about the resources. Information is essentially a kind of asset; sharing it, user nodes assist their potential competitors, in anticipation of their support in due course. Recent trends such as the smart city initiative [1] give rise to further settings, where truthful altruistic information sharing is required but not guaranteed. One of these settings, involving city-level parking assistance systems, is the subject of this paper.

In particular, advanced parking assistance systems have been proposed (*e.g.*, [2]), and in some cases realized (*e.g.*, [3] or [4], [5] via social networks), in an attempt to cope with the issue of parking space management in busy urban environments [6]. Fostered by recent advances in wireless networking, sensing and car navigation technologies have, these systems aim at helping drivers find vacant parking spots easier and faster by collecting and sharing information about the location and status (occupied/vacant) of parking spots. In *centralized* systems, a central server communicating with sensors at the parking spots coordinates the parking spot assignment process, by receiving the drivers' requests, reserving parking spots, and directing drivers thereto (*e.g.*, [7]). Whereas, in *opportunistic* systems, vehicles themselves serve as mobile sensing platforms that collect and store information about the location and status of parking spots and share it with other vehicles through vehicle-to-vehicle (V2V) communication technologies (*e.g.*, in [8]). Opportunistic systems do not incur the upfront infrastructure cost of centralized systems, thus presenting a lighter and more scalable solution that leverages to-be-built-in vehicle equipment. On the other hand, opportunistic systems lack central coordination and rely on the drivers' willingness to share collected information. This cannot be taken for granted since the sharing of information assists nodes by increasing their knowledge about parking space availability but, at the same time, *synchronizes* nodes' parking choices. This synchronization in turn increases the competition for the vacant parking spots, in particular when drivers' travel destinations overlap [9].

In this paper, we are, to the best of our knowledge, the first to question the robustness of opportunistic parking assistance systems to non-cooperative drivers' behaviors, which deviate from the purely *altruistic* paradigm of always *truthfully* sharing the cached information with encountered vehicles. Hence, we let nodes *misbehave* and study how this affects fundamental performance indices such as the parking search time and the distance of the acquired parking spots from the drivers' travel destinations. The dual question from a driver's viewpoint is whether nodes *do* have incentives to misbehave in that misbehaving lets them achieve better search times and/or parking spot-destination distances. Two intuitive instances of misbehaviors are considered. In the first one nodes defer from sharing parking information with other vehicles essentially acting as *free riders*. In the second one, they deliberately falsify information about the parking spots' status (*selfish liars*), *i.e.*, spots close to a misbehaving vehicle's destination are advertised as occupied whereas all others as vacant. The two misbehaviors essentially impair in different manner the *amount* and *accuracy* of information that is disseminated across the network.

The problem under consideration features strong spatiotemporal dynamics that are not conducive to theoretical investigation. Hence, the study is carried out primarily through simulations, whereas modeling is occasionally used to make theoretical arguments about the simulation findings. The results do not lie always in line with intuition. Notably, in almost all cases misbehaving nodes fail to obtain distinctly better performance than cooperative nodes. Both types of misbehavior, through different mechanisms, tend to reduce the destination-spot distances and increase the parking search times for *all* vehicles, the latter increase becoming quickly prohibitive when drivers' destinations overlap. This *fate-sharing* effect essentially weakens vehicles' incentives to misbehave and increases the system resilience to selfishly-thinking drivers. On the other hand, neither of the two misbehaviors attenuates the *synchronization phenomena* emerging at the cache contents, and subsequently, the mobility patterns of vehicles when their destinations overlap. The introduction of mobile storage nodes in this case, which collect and share parking information with parking-seeking vehicles, has a sharply different impact on the two misbehavior instances. Whereas, in the presence of free riders, a few of them suffice to restore the information flow at the levels of a cooperative system, they have negligible impact in the presence of selfish-liars: even a few misbehaving vehicles suffice to overwrite the fresh information mobile storage nodes carry and convert them into relays of forged information (*bona fide mules*).

The basic operation of the opportunistic parking assistance system and the two obvious ways selfish nodes may try to manipulate it are reviewed in Section 2. The simulation environment and our methodology are described in Section 3. We present and discuss the simulation results in Section 4, outline the related research in Section 5 and conclude our work in Section 6. Finally in Annex I we give a short review and taxonomy of misbehaviors and adversary profiles that can harm the nominal operation of Vehicular Ad hoc Networks.

2. OPPORTUNISTICALLY ASSISTED PARKING SEARCH AND IMPERFECT COOPERATION

According to the current common practice in search for parking space, drivers wander around their travel destination and sequentially check the availability of encountered parking spots. Typically, the search is initially carried out within an area around the drivers' travel destination (*initial parking search area*), whose size depends on the drivers' attitude and sense of traffic load and parking demand thereby. The radius of the search area then grows progressively as parking search time increases until drivers find a vacant parking spot and occupy it. This, essentially *blind*, search practice gives often rise to congestion problems and results in fuel/time wastage, especially around popular travel destinations such as the centers and business districts in big cities.

Recent progress in wireless communication, sensing and navigation technologies promise to make the parking search process smarter and more efficient. One way to do this is by equipping vehicles with sensors and standard wireless interfaces (*e.g.*, 802.11x) in ad-hoc mode that let them collect and share information about parking spots' location and status as they drive around. Such information can be further filtered across time (*aging*) and space through the use of timestamps and the geographic addresses (*e.g.*, via GPS) of individual parking spots. With such information at hand, vehicles can make more informed decisions. Rather than wandering randomly in the parking search area, a vehicle can now direct its search towards selected parking spots that are listed in its cache as the closest vacant ones to its travel destination. If the spot is actually vacant when it arrives at it, it occupies it; otherwise, it repeats the spot selection process, being also prompt to occupy any vacant spot it may find on its way to the candidate spot.

Critical for the efficiency of this *opportunistically-assisted* parking search are the *amount* and *accuracy* of the information that is stored in the vehicles' caches and shared among them. Both are subject to strong spatiotemporal effects: vehicles generally possess partial rather than global information about parking space availability and as the status of parking spots changes over time, stored data are potentially outdated after some time interval. Moreover, vehicular nodes have good reasons to hide information from other, potentially competitor, vehicles. Overall, the processes of information dissemination (benefiting discovery of parking spots and their availability) and competition growth (reducing the chances to acquire a spot) are coupled and counter-acting. Indeed, the faster information circulates across the wireless opportunistic networking environment, the more similar (accurate or not) data are stored in the caches of vehicles. Thus, depending on the travel destinations of users, the movement patterns of individual vehicles get synchronized and sharpen the effective competition for given parking spots [9]. This additional level of competition, this time for information at the "service discovery" level, motivates various deviations from the perfectly cooperative (altruistic) behavior.

In this paper, we consider in detail two variants of imperfect cooperation, hereafter called misbehaviors for the sake of brevity. In the first variant, misbehaving nodes defer from sharing their own information with other vehicles, while readily accepting such information from other vehicles that make it available. These free riders reduce the amount of disseminated information but also its accuracy since vehicles' caches are less frequently updated with fresh information about the spots' occupancy status. On the contrary, the second misbehavior instance involves the dissemination of falsified information about the status of parking spots. Nodes do so in order to create zones free of competition around their travel destinations by diverting encountered vehicles away from them. Compared to the first misbehavior instance, this one affects only the accuracy of the disseminated information.

Inferring *a priori* the impact of these rather common misbehaviors is not straightforward for two main reasons. The first one is the aforementioned spatiotemporal effect. For example, misbehaving nodes that forge information may inadvertently correct outdated information (*i.e.*, turn the availability status of the advertised parking spots to their real up-to-date value) and, thus, end up assisting the process. The second reason relates to the cache synchronization effects that emerge as the frequency of information updates rises. It may be argued that the two types of misbehaviors can serve as regulators for the synchronization phenomena and the resulting competition. We explore these aspects in detail in Section 4.

3. PERFORMANCE EVALUATION METHODOLOGY

3.1 Simulation Environment

Our study is carried out in the simulation environment developed for [9]. In what follows, we outline its features that are critical to our study.

Road grid and parking spots: The simulator implements a grid of two-lane roads (one lane in each direction) with roundabouts connecting up to four roads. Parking spots are uniformly distributed across roads' lanes of the grid.

Vehicle movement: The vehicle mobility model comes under the broad category of behavioral mobility models. Two levels of behavior can be identified: the *global*, determining how destinations are selected and the way the vehicles choose the route towards them; and the *local*, addressing how the vehicle moves within the roads comprising the route.

At the global level, every time a vehicle frees a parking spot, it chooses a new destination (geographical coordinates within the bounds of grid) and drives towards it. Once it reaches adequately close to the destination (*initial parking search area*), the parking search process is initiated. The initial parking search area is circular; it is centered at the travel destination with radius equal to half the distance between two adjacent intersections. Where the vehicle drives next depends on the information stored at its memory. The stored records (parking spot, status, timestamp) are filtered both temporally, to exclude information that is outdated (*i.e.*, coupled with a timestamp that is beyond a threshold value), and spatially, to retain as candidates only spots in the current search area. Out of the remaining spots, the user picks up the nearest-to-her-destination available one (*Full use of Memory, FM*). If no record survives the spatiotemporal filtering step, the driver chooses randomly one spot within the parking search area and moves towards it (*Random use of Memory, RM*). In the absence of *any* information about parking spots within the current area of interest, the vehicle circulates blindly/randomly within the area (*No Memory, NoM*). In all cases, vehicles move along shortest routes to their destinations and occupy the first available parking spot on their way to them rather than pursing closer-to-destination, yet non-guaranteed, parking options. If the driver finds a spot vacant, either a memory-selected or a randomly met one, it occupies it for a time interval (*parking time*) that may follow different probability distributions. By the end of this interval, she vacates the spot and selects another destination. Otherwise, upon a failured attempt, the user will check anew her memory and repeat the attempt, as aforedescribed. After a particular number of failured attempts in the current parking search area, the driver increases its range.

At local level, the position of each vehicle by the next simulation time step depends on its current position and velocity. More specifically, the vehicles adapt their speed according to their distance from: (a) the front vehicles (they are not allowed to overtake one another); (b) the next intersection; and (c) the nearest parking spot, assuming that they decelerate when encountering parking spots to check their status. Their speed is zeroed when they get stuck in traffic jam, enter a roundabout intersection, or park. Finally, the vehicles are not allowed to stop or move in the reverse direction of the traffic flow.

Cooperative *vs.* misbehaving vehicles: All vehicles inform their memory cache every time they hit a parking spot sensor. Well-behaving (cooperative) vehicles *share truthfully* stored information about the location and status of parking spots each time they encounter other vehicles. On the other hand, misbehaving vehicles realize the two misbehavior instances described in Section 2:

Information Denial: Upon encounters with other nodes, they suppress information they store about the location and availability of parking space, whereas they update their cached information with all the new knowledge offered. During their search, they use the cached information the same way as cooperative nodes.

Information Forgery: They advertise all parking spots within a specific distance from their destinations (*Radius of Interest, RoI*) as occupied, and all others as vacant, while setting the relevant timestamps to fresh values. Being more suspicious about falsified information, they persist more when searching around their destinations; namely, they run additional random trips (in the RM or NoM mode) over the initial parking search area before they decide to increase the range of their search.

3.2 Simulation set-up and performance metrics

Unless otherwise stated, the simulations are run with the parameter values (value ranges) shown in Table 1.

Performance Metrics: The two main performance metrics throughout our study are the average time spent for searching available parking place (*Parking search time,* T_{ps}) and the average geographical distance between the vehicles' travel destinations and the selected parking spots (*Destination - parking spot distance,* D_p). In addition, at a more microscopic level, we extract results for the profile of the information that is stored at vehicles' caches as well as the way vehicles use it and benefit from it, by plotting statistics about the percentage of time (total efforts) the vehicles search in *FM* and *RM* mode.

Table 1: Simulation parameters

Parametres	**Values**
Simulation Area	1200 x 1200 m^2
Simulation Time	100000 sec
Number of uniformly distributed spots, P	25
Number of vehicles , V	5-70
User maximum speed	14m/s ~ 50 km/h
Vehicle – spot sensor commun. range	15m
Vehicle – vehicle commun. range	70m
Exponential parking time with mean	1800 sec
Distance between adjacent roundabouts	300m
Linear increase step of parking search area	150m
Radius of Interest, RoI	150, 350, 500m
Ratio of misbehaving nodes, p	**0, 0.3, 0.5, 0.8, 1**

4. SIMULATION RESULTS - EXPERIMENTATION

In all plots, we compare the metric values under perfectly cooperative operation with those under different misbehavior intensities for various levels of parking demand. Each point in the plot results from averaging parking events over either the full set of nodes, or, separately, cooperative (denoted by 'C') and misbehaving (non-cooperative) ones (denoted by 'NC'). Drivers are assumed to be persistent in their search. Alternatively, they could abandon their effort to park, *e.g.*, stop looking for on-street parking and head for a more expensive parking lot, once the parking search time exceeds an upper bound. A red line in the plots indicates a timeout for the parking search process at 1800 seconds.

4.1 Uniformly distributed travel destinations

4.1.1 Information Denial

The first remark out of Figures 1, 2, 3 is that the system exhibits remarkable robustness to this type of misbehavior. Neither the average parking search time (Fig. 1) nor destination-spot distance (Fig. 2) are penalized even when half the vehicular nodes defer from sharing information. An increase in parking search time becomes visible when 80% of the nodes misbehave and evolves to a striking tradeoff when all nodes misbehave; namely, if all vehicles defer from information sharing, they end up acquiring spots closer to their destinations at the expense of higher search time. The reason for this can be traced in the combination of Fig. 3 and Fig. 4. Without information sharing, the caches of nodes are primarily populated with records of spots around their travel destination (initial parking search area), encountered during their very first attempts. As these spots are occupied (for medium-to high demand), and although vehicles gradually increase the range of their search, they still end up randomly selecting one of these spots with high probability (search in RM mode). Contrary to when even a few nodes share information (Fig. 3), their caches are not refreshed with records of more distant spots communicated by other vehicles. Instead they are only occasionally enriched with some randomly encountered spot in the destination proximity, where their search ends up being restricted. Reading the system robustness the other way round, equally remarkable is the failure of selfishly misbehaving nodes to attain better performance, when compared to what cooperative nodes achieve (ref. to ingraphs in Fig. 1 and Fig.2).

On the other hand, Figures 4, 5, 6, 7 give clear insights to a fundamental inefficiency of opportunistically-assisted search, the coupling of information sharing (about parking spots) with the generated competition (*for* parking spots). The ratio of searching attempts in FM mode (Fig. 5), starts from low levels at small demand, where anyway it is easier for a vehicle to find a spot and decreases as the number of competing vehicles grows, where more spots are occupied, more vehicles are parked, and the flow of information is yet too slow enough to fill the vehicles' caches with adequately fresh information about vacant spots. When the demand grows even more and more vehicles end up cruising around, the information flow (at least for moderate intensity of misbehavior) is strengthened. Vehicles find fresh records about vacant spots at their caches, yet these are only a few and the competition for them so sharp that this information rarely results in a successful attempt (Fig. 6, 7) For higher intensity of misbehaviors, both the frequency and success rate of search in FM mode decrease.

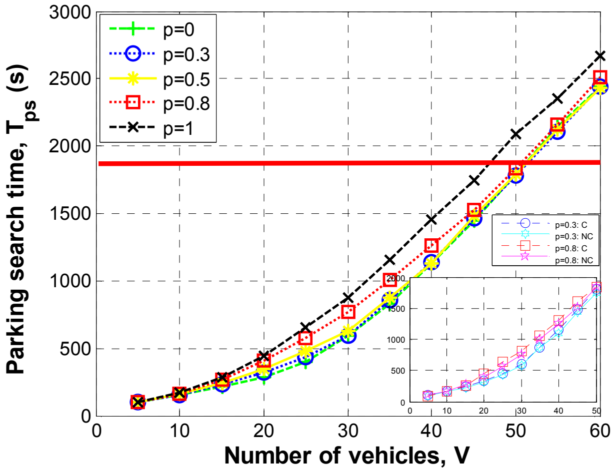


Figure 1: Average parking search time

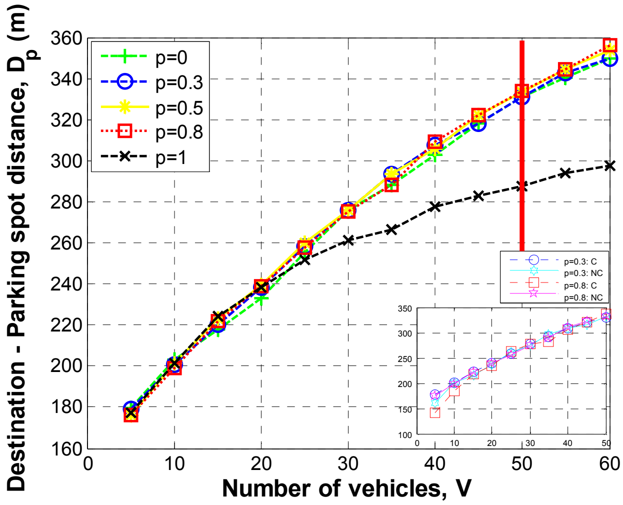


Figure 2: Average destination-spot distance

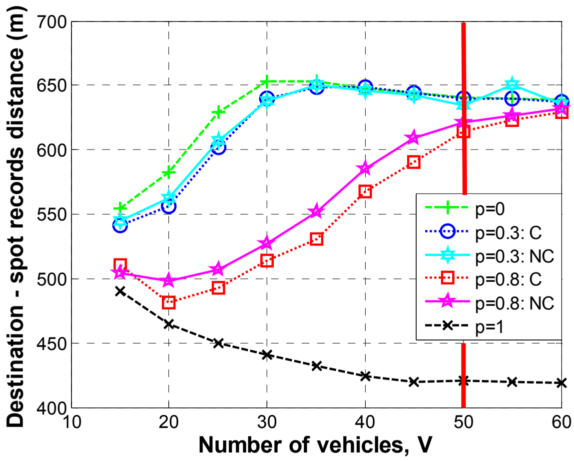


Figure 3: Average distance from destination of spot records at vehicles' caches

Figures 1, 2, 3: Robustness of the opportunistically assisted parking search to *Information Denial*: uniformly distributed destinations

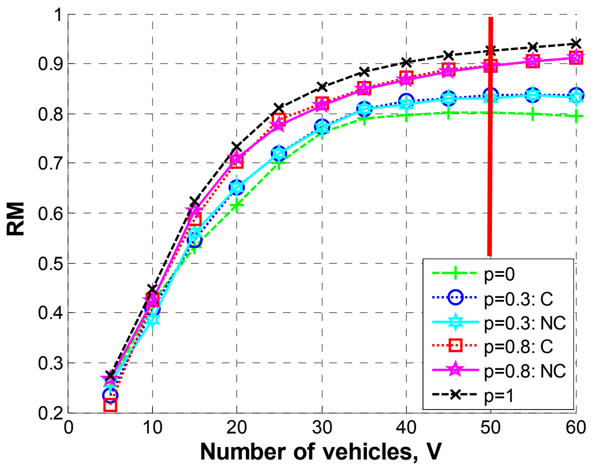


Figure 4: Ratio of parking attempts in RM mode

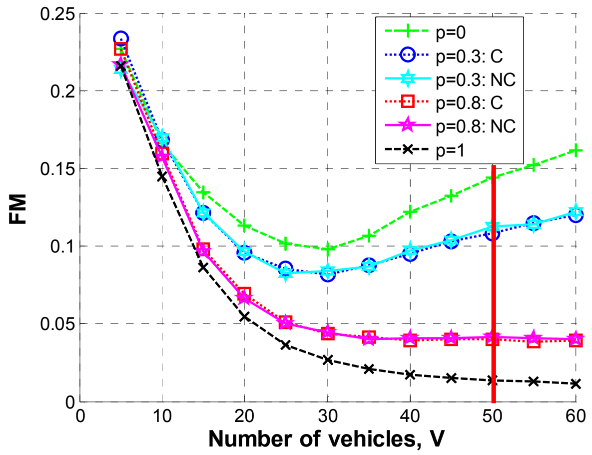


Figure 5: Ratio of parking attempts in FM mode

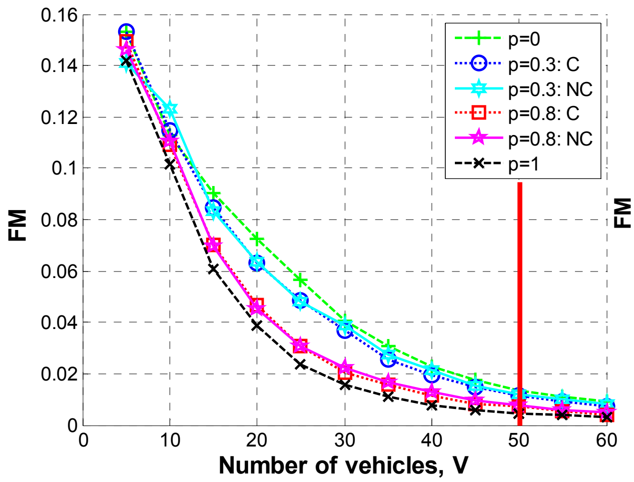


Figure 6: Ratio of successful parking attempts in FM mode

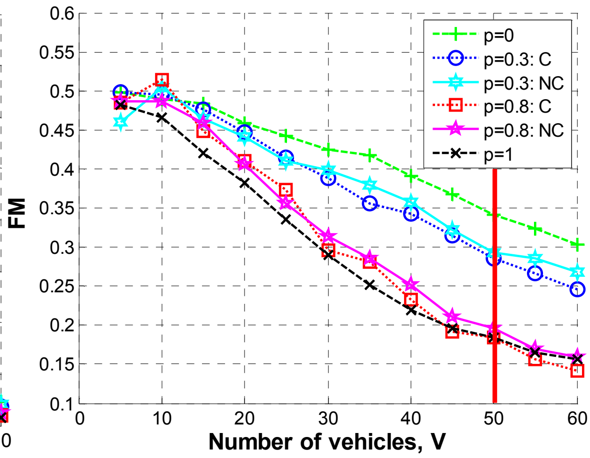


Figure 7: Ratio of successful parking attempts in FM mode over all successful attempts

Figures 4, 5, 6, 7: Search mode and parking attempt success rates under *Information Denial*: uniformly distributed destinations.

4.1.2 Information Forgery

Under Information forgery, the vehicular nodes try to spontaneously generate competition-free zones around their travel destinations. For small RoI values, these zones are narrow and disjoint. Since misbehaving nodes advertise parking spots outside these zones as vacant and the drivers' destinations are uniformly distributed, the (cooperative) nodes end up (incorrectly) listing spots around their own travel destinations as vacant for most of the time. These spots emerge as top choices out of the spatiotemporal filtering step (FM mode) and attract repeated vehicles' parking attempts (Fig. 10). As a result, the vehicles park closer to the destination at the expense of higher search times. As misbehaving nodes become more aggressive and the zones they try to induce start to overlap (*RoI* = {350; 500}), most spots at the vehicles' caches are reported as occupied, the vehicles exercise more the RM mode, and a tradeoff emerges between destination-spot distances and parking search times, as shown in Figures 8, 9.

Contrary to the Information Denial misbehavior, under Information Forgery the misbehavior intensity and its impact do not only depend on the number of misbehaving nodes but also on the population of cooperative nodes. The latter inadvertently propagate forged information across the network once they get infected with it upon encounter with a misbehaving node. This has two direct consequences. First, the destination-spot distance *vs.* parking search time tradeoff is now milder as shown in Figures 11, 12; for given *RoI* even a small ratio of misbehaving nodes suffices to populate the vehicles' caches with supposedly vacant spots and steer their attempts to spots around their travel destinations (Fig. 13). Secondly, with a small exception low parking demand levels ($V < P$), misbehaving nodes cannot gain any substantial performance advantage over cooperative nodes (ref. to ingraphs in Figures 8, 9, 11, 12) since the manipulated information they generate, bounces back to them after one or more hops over cooperative nodes. This *fate-sharing* effect essentially mitigates the incentives of nodes to misbehave.

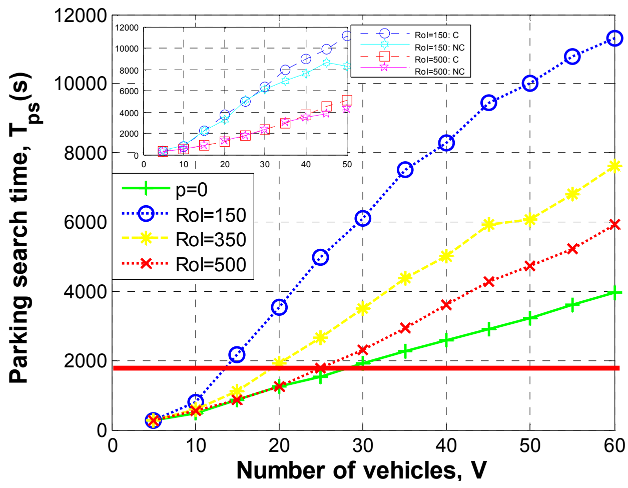


Figure 8: Average parking search time

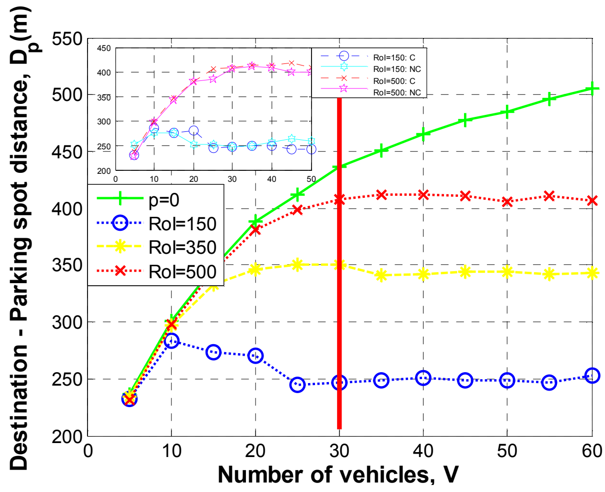


Figure 9: Average destination-spot distance

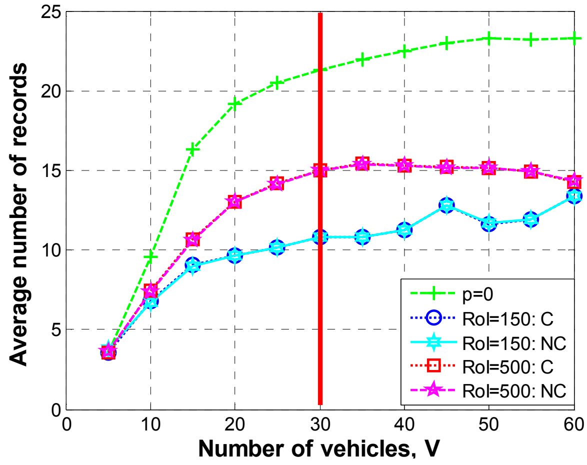


Figure 10: Ratio of parking attempts in FM mode

Figures 8, 9, 10: Robustness of the opportunistically assisted parking search to *Information Forgery:* uniformly distributed destinations, *p* = 0.3

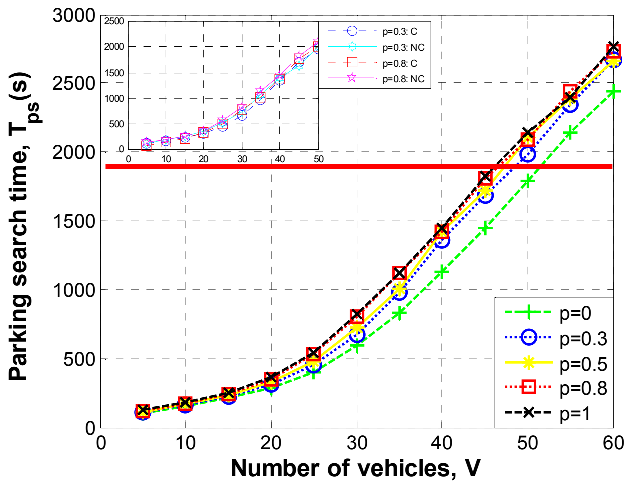


Figure 11: Average parking search time

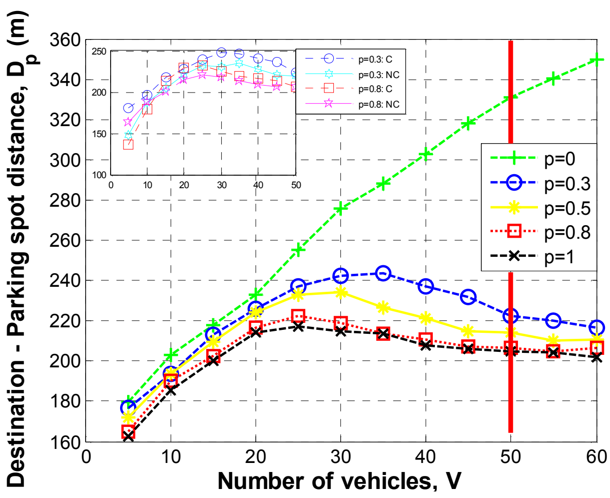


Figure 12: Average destination-spot distance

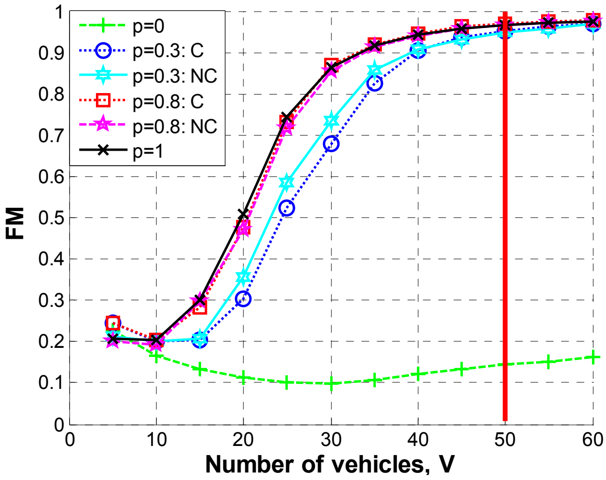


Figure 13: Ratio of parking attempts in FM mode

Figures 11, 12, 13: Robustness of the opportunistically assisted parking search to *Information Forgery:* uniformly distributed destinations*, RoI* = 150

4.2 Hotspot Scenario

Under a fully cooperative setting, the spatial concentration of vehicles' travel destinations has two direct consequences on the information stored at their caches. First, as all vehicles cruise along the hotspot area and encounter each other more frequently, they tend to synchronize their caches with records about the same set of spots. Secondly, and most importantly, they rank these spots identically. Hence, at least as long as drivers let the system direct their attempts, their trips get synchronized, competition sharpens and parking search times increase substantially [9].

4.2.1 Information Denial

In the hotspot setting, the Information Denial has a double-edged effect. On the positive side, the system is shown to be resilient to the free-rider behavior; even when half the nodes defer from sharing information, the average parking search times and spot-destination distances are almost intact, as shown in Fig. 14 and Fig. 15, respectively. Furthermore, misbehaving nodes do not gain in both performance indices by hiding information (ref. to ingraphs in Fig. 14 and Fig. 15). On the other hand, this misbehavior does not manage to break the inherent synchronization effects and drive the system to a better-than-nominal performance level. When eventually, with most nodes in the network misbehaving, differentiation is achieved at the vehicles' caches, it is outweighed by a substantial decrease of disseminated information. Vehicles do not get informed about and do not take advantage of vacant parking spots further away from their common destinations (Fig. 16). They rather end up parking closer to them, yet at the expense of unacceptable cruising times, even under moderate parking demand levels.

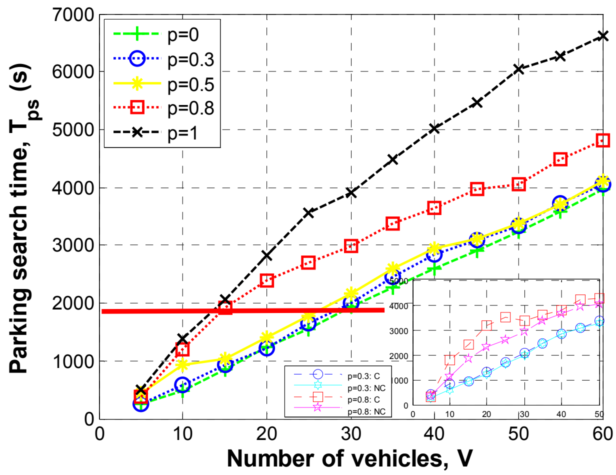


Figure 14: Average parking search time

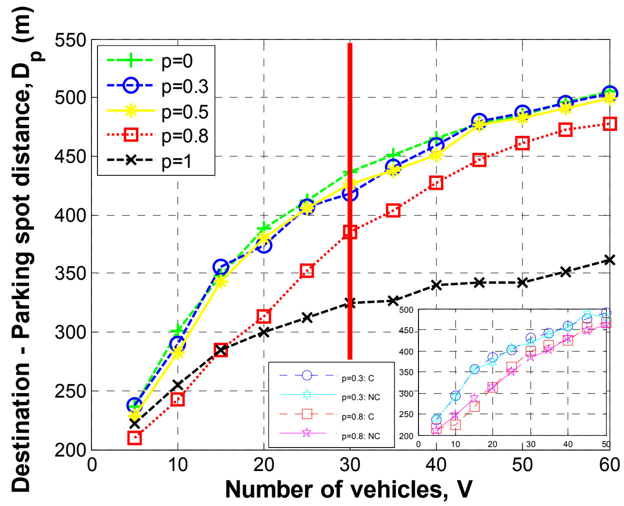


Figure 15: Average destination-spot distance

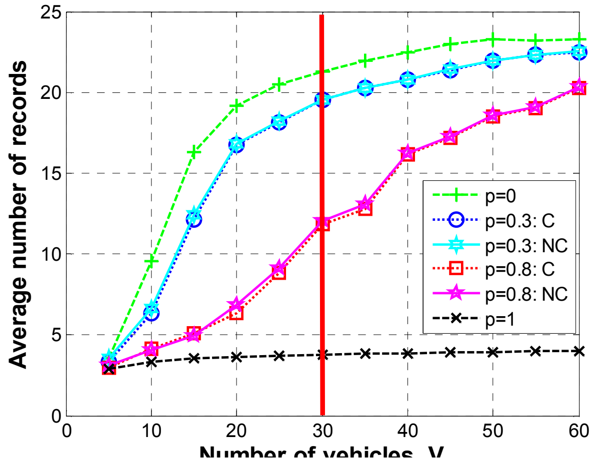


Figure 16: Average number of records in memory

Figures 14, 15, 16: Robustness of the opportunistically assisted parking search to *Information Denial:* hotspot road.

4.2.2 Information Forgery

In the hotspot scenario, the zones that misbehaving vehicles try to clear from competition overlap and all vacant spots beyond a distance equal to RoI are advertised as vacant by misbehaving nodes. For small RoI, vehicles persistently direct their attempts towards the few spots lying close to their common destinations so that their caches are not enriched with information about vacant spots further away, as shown in Fig. 19. The synchronization/competition effect is stronger and vehicles waste even more time in myopically searching for a parking spot around the hotspot road (Fig. 17). However, as a result of this search mode, the vehicles park closer to their destination (Fig. 18). Interestingly and rather counter to intuition, as misbehaving nodes become more aggressive and try to clear from competition larger areas (*i.e.*, *RoI* = *{*350*;* 500*}*), the parking search times improve for all vehicles. The reason is that vehicles are steered by the content of their caches to expand their search further away from the hotspot area and have the chance to encounter and, potentially occupy, spots they were not aware of. Essentially, the movement of vehicles in a broader area helps alleviate, though not resolve, the synchronization effect. Again, as with uniformly distributed travel destinations, misbehaving nodes cannot attain some performance advantage since the falsified information returns back to them after a few encounters with other nodes, this time even faster due to more frequent encounters between vehicles (ref. to ingraphs in Fig. Figure and Fig. Figure).

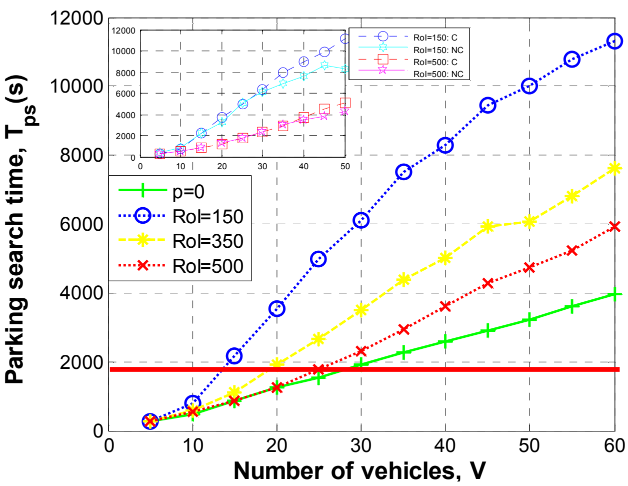


Figure 17: Average parking search time

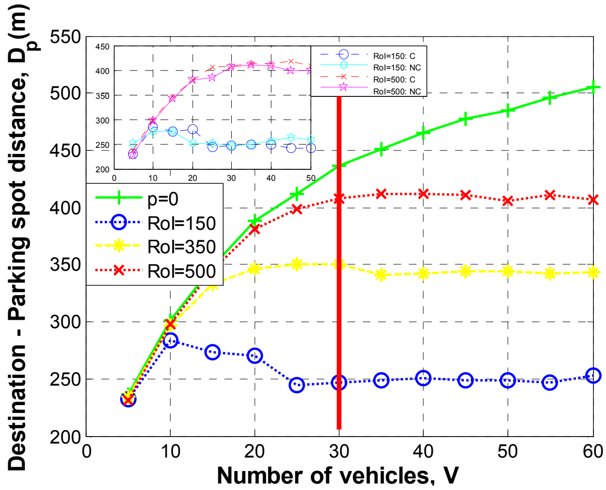


Figure 18: Average destination-spot distance

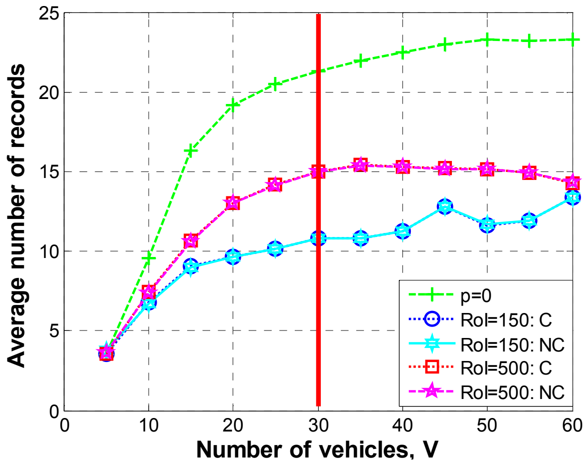


Figure 19: Average number of records in memory

Figures 17, 18, 19: Robustness of the opportunistically assisted parking search to *Information Forgery:* hotspot road.

4.3 Mobile Storage Nodes for the hotspot scenario

The Mobile Storage nodes (MSNs) can be either dedicated or normal vehicular nodes, *e.g.*, city cabs, equipped with wireless interfaces that allow them to collect parking information from the entire area and share it with other vehicles and MSNs. By relaying information, MSNs indirectly increase the effective contact opportunities between vehicles and thus, the speed of the information spread. The efficiency of MSNs as a countermeasure for the two types of misbehaviors is very different.

4.3.1 Information Denial

In this case, even a very small number of MSNs restore the information flows at the levels (and even better) of the fully-cooperative system. They render both the average parking time and the spot-destination distance independent of the number of free-rider vehicles, as can be clearly seen in Fig. 20, 21. Even when vehicles do not exchange at all information with each other, the communication with MSNs suffices to achieve better parking search times than those under the fully cooperative system. The addition of more MSNs (we experimented with 15 MSNs) does not bear visible changes to the performance metrics; on the other hand, similar results are obtained with even one MSN. In fact, a single encounter with MSN informs nodes about *all* parking spots in the area, helping them expand their search in a broader area around the hotspot road and partly randomize their driving patterns. Yet, the synchronization phenomena due to the vehicles' overlapping travel destinations are not fully eliminated and retain the parking search times at significantly higher levels than under uniformly distributed destinations.

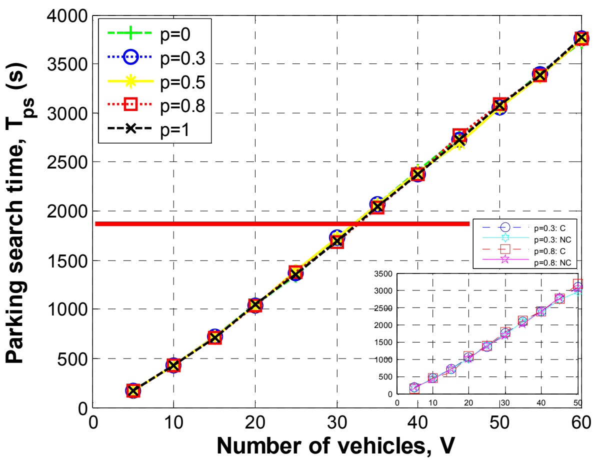


Figure 20: Average parking search time

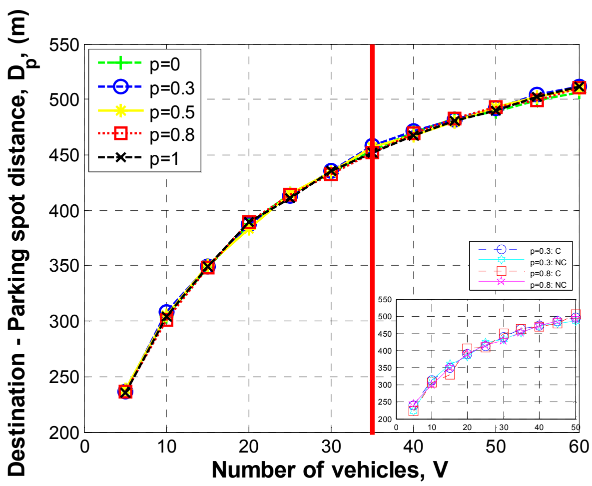


Figure 21: Average destination-spot distance

Figures 20, 21: MSNs and *Information Denial*: hotspot road.

4.3.2 Information Forgery

When nodes misbehave this way, the MSNs are a far less efficient solution. Although they collect and store up-to-date information about the actual status of parking spots as they move randomly within the grid, this information is *rewritten* upon encounters with misbehaving nodes (or even otherwise cooperative nodes that have been polluted with falsified information). Thus, MSNs end up further fostering the diffusion of falsified information that synchronizes the vehicles' caches making the synchronization effects even stronger and the decrease of the search times thanks to additional fresh information, marginal (Fig. 22, 23).

The (non-) efficiency of MSNs in coping with selfish liars can be interpreted through a simple model of interacting objects. The model does not intend to capture the exact interaction of vehicles in the hotspot scenario but rather the essence of the emerging synchronization effects. Let S and C be the populations of two classes of network nodes, stubborn (*i.e.*, selfish) and conciliatory (*i.e.*, cooperative), respectively, with $S + C$

= *N*, and *Z* a physical location in the network, whose state at any point in time is a binary variable $\in \{0,1\}]$. Assume also that pairwise node encounters form uniform Poisson processes of rate λ and that all nodes hit *Z* with Poisson rate *h*. Stubborn nodes persistently advertise that *z* is in state 0; whereas, conciliatory nodes update their information about *z* upon two kinds of encounters. Whenever they meet a stubborn node, they adopt what it states about *z*, *i.e.*, *z* = 0. In parallel, they may themselves hit *Z* and update their knowledge about its state. When nodes of the same type encounter each other, they do not update their information but rather stick to what they know. If $x_1(t), 0 \leq x_1(t) \leq N - C$ denotes the number of nodes over time, whose information about *z* is *not* in sync with what the *S* nodes propagate, then its evolution over time is a stochastic process coming under the broader family of density-based Continuous Time Markov processes. Drawing on the mean-field theoretic arguments in [10], the evolution of $E[x_1(t)]$ for large *N* can be approximated by the deterministic solution of the ordinary differential equation (ODE).

$$\dot{x}(t) = h\big(C - x(t)\big) - \lambda S x(t) \qquad (1)$$

This is a first-order linear ODE with initial condition $x(0) = C = N - S$ and solution

$$x(t) \doteq E[x_1(t)] = \frac{N-S}{\lambda S + h}\left[h + \lambda S e^{-(h+\lambda S)t}\right] \quad (2)$$

Namely, the average number of nodes that maintain their own assessment of the status of *z* reduces over time to $\frac{(N-S)h}{h+\lambda S}$.

Now, consider adding to the network *R bona* fide storage nodes relaying information about *z*. When a storage node encounters a stubborn node, it synchronizes with it, and when it encounters a conciliatory node, it propagates its own information on it. Essentially, the three types of nodes form a three-level hierarchy regarding their capacity to impose their information, with conciliatory nodes at the bottom level and stubborn ones at the top level. If $x_1(t), x_2(t)$ denote the number of conciliatory and storage nodes, respectively, that are not in sync with the stubborn nodes, their evolution over time is a two-dimensional Markovian process and, with similar arguments as before, it can be approximated by the deterministic solution of the non-linear system of ODEs

$$\dot{x}(t) = \big(C - x(t)\big)h - x(t)(R+S)\lambda + \lambda C y(t) \qquad (3)$$

$$\dot{y}(t) = -y(t)(h + \lambda S) + hR \qquad (4)$$

with initial values *x*(0) = *C* and *y*(0) = *R*. Solving initially the first-order linear ODE for *y*(*t*) and replacing to obtain another first-order linear ODE for *x*(*t*), we obtain:

$$x(t) \doteq E[x_1(t)] = \frac{N-S}{h+\lambda S}\left[h + \lambda S e^{-(h+\lambda S)t}\right]$$

$$y(t) \doteq E[x_2(t)] = \frac{R}{h+\lambda S}\left[h + \lambda S e^{-(h+\lambda S)t}\right] \qquad (5)$$

The expression for $E[x_1(t)]$ coincides with that without storage nodes in (2). Hence, the mobile storage nodes do not really alter the dynamics, through which stubborn (*a.k.a.* selfish) nodes synchronize the conciliatory (*a.k.a.* cooperative) nodes to their (deliberately falsified) information.

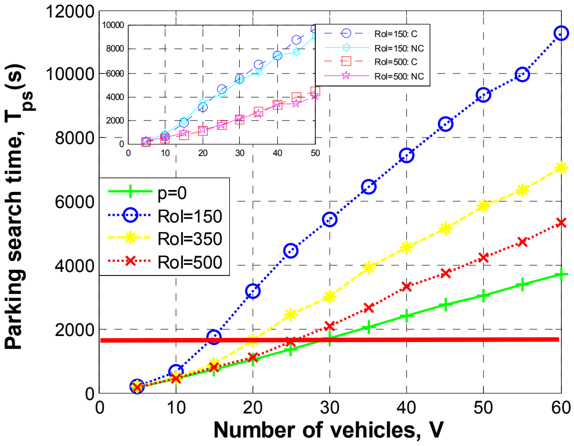


Figure 22: Average parking search time

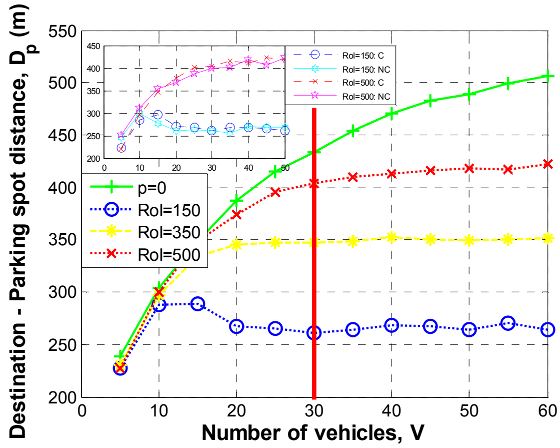


Figure 23: Average destination-spot distance

Figures 22, 23: MSNs and *Information Forgery*: hotspot road.

4.4 Centrally assisted parking search

In this work, our research interests focus primarily on the lighter and more scalable opportunistic parking assistance systems. However, partial or no cooperation of vehicles/drivers is a concern for both the opportunistic and centralized systems. Indeed, drivers' compliance seems extremely doubtful in a centralized parking spot allocation scheme. However, the detection and penalization of misbehaviors in an infrastructure-based system is not only challenging but expensive as well. For instance, the established fixed sensor networks need to function not only to monitor the parking space availability but also confirm the legitimate parking events (and thus support billing). Furthermore, the centralized systems' supervisory mechanisms need to either implement barrier-controlled metered parking spaces or enforce penalties in a pervasive sensing road platform.

In an effort to explore the way node misbehaviors shape the performance of centralized approaches, we implement scenarios with misbehaving nodes in the centralized system paradigm developed for [9] when all travel destinations are uniformly distributed. Nodes under nominal operation and parking sensors in centrally assisted parking search system transmit to the server parking requests specifying their destination and spot vacancy information, respectively. In a First-Come-First-Served (FCFS) manner the server queues the requests and satisfies them, reserving for the vehicle the closest vacant spot to its destination. When user is notified about the reservation, moves towards it and while waiting an answer from the system circulates blindly within the area.

This kind of systems is open to *position stealing* attacks/misbehaviors. The prospective *stealer* doesn't strictly follow the spot's assignment system process and constantly seeks for a better parking place. Specifically, if the stealer encounters a vacant spot while moving randomly waiting for the system assignment, occupies it. Likewise, the stealer bypasses server's directions, while driving towards the spot that the system reserved for her; namely if she detects a vacant spot located closer to her destination than the assigned one, she occupies it. Otherwise, she keeps driving to her initial destination.

Looking at Fig. 24, 25, 26, one can notice that this type of misbehavior cannot affect system performance regardless of the intensity of misbehaving nodes. Neither average parking search time (Fig. 24) nor destination-spot distance (Fig. 25) differ from the full altruistic scenario (p = 0). Additionally, no difference is observed in the number of parked vehicles for different ratios of misbehaving nodes, verifying the high robustness of centralized systems with respect to the position stealing misbehavior (Fig. 26). Despite misbehaving vehicles' efforts to gain performance advantage acting selfishly, on average, they end up parking to spots equally attractive to what the system has reserved for them: for P<25, the is no need to steal a spot since the system serves vehicles' requests in an optimal way; for P>25, the stealing efforts are scarce since the demand is high and hence, the possibility to encounter a vacancy is very low.

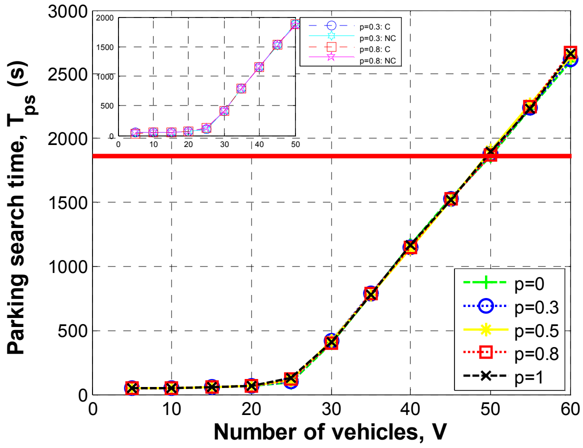


Figure 24: Average parking search time

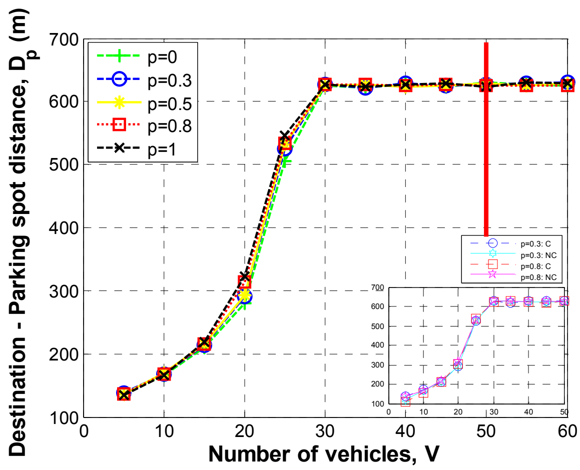


Figure 25: Average destination-spot distance

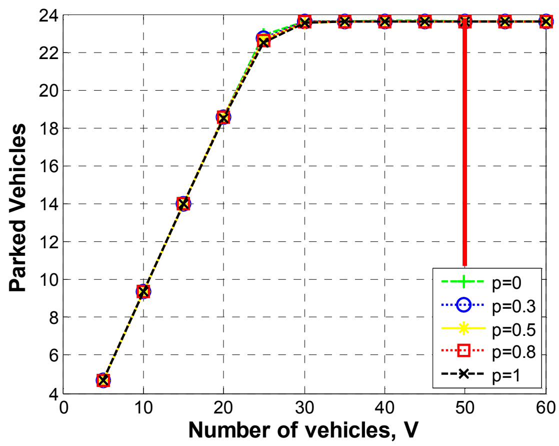


Figure 26: Number of parked vehicles

Figures 24, 25, 26: Robustness of the centrally assisted parking search to *Position Stealing:* uniformly distributed destinations

5. RELATED WORK

Misbehaviors and challenges in securing systems have been explored in the broader context of VANETs with respect to a wide range of safety, traffic management, and infotainment applications [11]. Primitives for secure applications and properties that can support secure systems are discussed in [12], [13]; while particular paradigms for authentication mechanisms and security protocols are presented in [14], [15]. Parking assistance applications lie at the intersection of traffic management and infotainment applications. *Opportunistic* parking assistance systems, in particular, are proposed in [8], [16] and [17]. In [8], a scalable information dissemination algorithm is presented where the vehicles are allowed to exchange aggregate parking information of variable accuracy. In a similar work, the vehicles exchange information and solve a variant of the Time-Varying Travelling Salesman problem while dynamically planning the best feasible trip along all (reported-to-be) vacant parking spots [16]. In a different approach, Delot *et al.* propose in [17] a distributed virtual parking space reservation mechanism, whereby vehicles vacating a parking spot selectively distribute this information to their proximity. Hence, they mitigate the competition for the scarce parking spots by opportunistically controlling the diffusion of the parking information among drivers.

Common to all these studies is that the parking assistance systems are proposed under the assumption of full cooperation of vehicles. To the best of our knowledge, our study is the first one that considers the impact of imperfect cooperation on the operation of opportunistic parking assistance systems. We have particularly focused on the ways different nodes may try to impede or manipulate the flow of information in order to better serve their own interests and whether the introduction of storage nodes may compensate for these misbehaviors.

6. CONCLUSION

The paper has looked into the vulnerability of opportunistic parking assistance systems to drivers' selfish behaviors. In our study drivers are let behave as free-riders that benefit from information other vehicles collect and share but do not share theirs; and selfish liars that falsify information at their caches in order to increase their chances to find a spot close to their destinations.

Interestingly and counter to intuition, our results reveal a persistent fate-sharing effect; namely the misbehaving nodes fail to obtain any substantial performance advantage over what the cooperative nodes achieve, irrespective of the distribution of travel destinations. On the contrary, misbehaviors tend to increase parking search times, sometimes (overlapping travel destinations) to unacceptable levels, and reduce the distance between parking spot and travel destination. Both misbehaviors deteriorate the synchronization phenomena that emerge with respect to the information stored by vehicles and their movement patterns when travel destinations overlap. Mobile storage nodes can compensate the impact of free-riders and improve the system performance beyond that of the fully cooperative scheme. On the contrary, they have almost no effect when confronting selfish liars since they end up propagating the falsified information those nodes generate. Further support to this result is provided by a simple model of interacting entities, which draws on mean-field theoretic arguments.

ACRONYMS

C	Cooperative
NC	Non Cooperative
FM	Full use of Memory
RM	Random use of Memory
NoM	No use of Memory
RoI	Radius of Interest
T_{ps}	Parking Search Time
D_p	Destination - Parking Spot Distance
MSN	Mobile Storage Node
ODE	Ordinary Differential Equation

ANNEX I

In the following paragraphs we present a short review and taxonomy of behaviors and adversary profiles that can harm the nominal operation of Vehicular Ad hoc Networks (VANETs).

A. VANETs

VANETs are networks consisting of independent nodes. which communicate with each other wireless in order to exchange messages about driving conditions or other information that might be useful to network nodes. Specifically, these nodes can be dedicated or normal vehicles and modules of the road-side infrastructure, such as traffic lights, bus stations or toll stations, on which wireless transceivers can be mounted. Communication in these networks is performed in two different ways.

Vehicle to Vehicle Communication (V2V): Information is shared between neighboring vehicles that are within the communication range of each other.

Vehicle to Infrastructure Communication (V2I): Direct communication is carried out between vehicles and the existing infrastructure.

On both occasions, nodes can operate as message creators, relays, or receivers; therefore, they should be equipped with transceivers (802.11 x), memories, GPS, navigation systems and specific range detection systems.

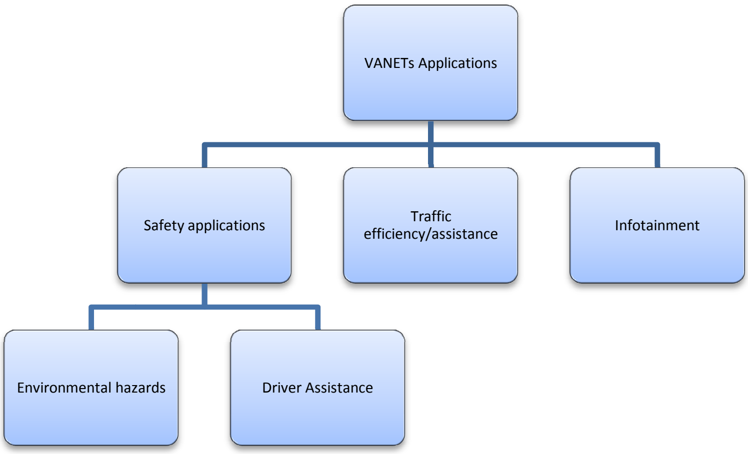
B. VANETs' Applications

VANETs support a range of applications with multiple benefits for their users. These applications can be divided to three major classes [12] as seen in Picture 1.

Safety applications: Safety applications contribute to safe and cooperative driving. Specifically, such applications warn drivers about dangers that might emerge due to environmental or driving conditions, i.e., presence of ice on the road, collision avoidance.

Traffic efficiency/assistance applications: Traffic efficiency/assistance applications are applications whose main purpose is to inform drivers for traffic conditions, for example the existence of traffic congestion ("Traffic congestion detection", [13]).

Infotainment applications: Infotainment applications offer entertainment and general information to drivers, i.e., search for gas stations, toll stations, ATMs.



Picture 1: VANETs' applications

Parking assistance systems can be considered either as traffic assistance or as infotainment applications.

C. Adversaries

VANETs are often prone to misbehaviors caused by nodes who seek to disrupt the network. Adversaries can be characterized by a) the motivation, b) the method and c) their impact of their actions on network operations.

Specifically, considering the motivation of the adversaries, we have identified the following categorization:

Malicious – Rational: A *Malicious (M)* node has no benefit or incentives, which justify her behavior; hence, this type of adversary cannot be easily predicted and modeled. Her only goal is to harm the network and network users. On the other hand, a *Rational (R)* node acts for personal gain and has more predictable behavior [14], [12].

Adversaries may also be classified according to qualitative features of their misbehavior into:

Active – Passive: An *Active (A)* node uses the transmission of packets, signals and messages to strike the network, while a *Passive (P)* node monitors the communication channel and has the ability to intercept messages [14].

Independent – Colluding: An *Independent (Ind)* node acts alone while a *Colluding (C)* one acts within a group seeking to cause problems in the network and its users [12].

Persistent – Random: A *Persistent (Per)* node hurts the network persistently while a *Random (Rm)* node may start or terminate her activity very suddenly [12].

The third distinction concerns the extent of the adversaries' impact on the network. Thus, their impact is characterized as:

Local – Extended: A *Local (L)* node affects many nodes that move in limited geographical area, unlike an *Extended (E)* one that expands the radius of its impact and harms nodes that are widely spread in the network [14].

An additional classification attribute is related to whether the misbehaving node is a certified member of the network or some node that has just invaded in the network:

Insider – Outsider: An *Insider (I)* node is a certified member of the network. Practically, this means that she has some kind of certified key that makes her automatically "trusted" for communication. An *Outsider (O)* node is a network's "invader" without certification. Thus, she lacks opportunities/means to harm network robustness in many different ways [14].

D. Profiles

Typically, the profiles of misbehaving nodes exhibit features from two or more adversaries' categories. Representative examples of nodes' profiles are [13]:

Greedy: (Insider or Outsider, Rational, Active, Local or Extended, Independent or Colluding, Persistent or Random). A Greedy node seeks to maximize the benefits from using the network regardless of the problems that she can cause to other users of the network.

Snoop: (Insider or Outsider, Rational, Passive, Local or Extended, Independent or Colluding, Persistent or Random). A Snoop node invades others' privacy, gathering their profile information.

Prankster / Malicious Attacker: (Insider or Outsider, Malicious, Active, Local or Extended, Independent or Colluding, Persistent or Random). Prankster / Malicious Attacker is the node that can cause network problems without any explicit reason. She acts maliciously for its own pleasure and causes extensive or limited damage. Moreover, a key feature of the action of such a node is that her behavior is unpredictable.

Industrial Insider: (Insider or Outsider, Malicious, Active, Local or Extended, Independent or Colluding, Persistent or Random). Industrial Insiders are considered the individuals who have the expertise to intervene in the software systems of the vehicles.

Table 2: Misbehaving nodes' profiles

Profiles \ Behavior	A	P	Ind	C	Per	Rm	M	R	L	E	I	O
Greedy	X		X	X	X	X		X	X	X	X	X
Snoop		X	X	X	X	X		X	X	X	X	X
Prankster/ Malicious Attacker	X		X	X	X	X	X		X	X	X	X
Industrial Insider	X		X	X	X	X	X		X	X	X	X

E. Types of Misbehaviors

Adversaries that intend to harm VANETs use several ways to achieve their goal. Their misbehavior may be categorized as follows:

Denial of Service: This kind of misbehavior occurs in two forms. According to one of them, the node interferes the communication channel in order to prevent message transmission within range (jamming). According to the second form, adversaries overwhelm vehicles' resources [14] [12] [13].

Forgery: Adversaries displaying this type of misbehavior transmit false information to other nodes of the network. In a typical example an adversary node disseminates false information about traffic in order to divert vehicular away from a particular area of own interest. Another example is the transmission of bogus messages about the existence of ice on the road [12].

Masquerading: In this type of misbehavior an adversary with selfish or malicious incentives pretends to be another vehicle using a false identity [14].

In-Transit Traffic Tampering: According to this type of misbehavior, adversaries that retransmit data affect the communication between nodes by losing, corrupting or meaningfully modifying messages. Probably these nodes disorientate their neighbors by retransmitting older messages, or updated messages about another area of the network [12].

On-board tampering: Adversaries adopting this type of misbehavior modify some parts of the transmitted messages that are associated with the position, direction, or speed of their vehicle [12]. For example, a node can exhibit this behavior in order to avoid taking responsibility for an accident that she has caused.

F. Mapping of misbehaviors to applications

As mentioned above, applications offered by VANETs are divided into three categories. Each one of these categories is more sensitive to certain types of misbehaviors. Therefore, in this section we present a mapping of misbehaviors to those applications that they hurt in a greater scale.

Safety applications: Using these applications, drivers can get informed about environmental and driving conditions that may affect their safety. Safety messages' dissemination rate should be high enough to prevent malfunction in the network that can be caused by network interferences or transmission of useless and forged messages. So, safety applications are more vulnerable to *denial of service*, *forgery*, *in-transit traffic tampering* and *on-board tampering*.

Traffic efficiency: In these applications drivers are informed about traffic conditions in the network. So, misbehaviors that can cause serious problems in this case are the ones associated with transmission of false or exaggerated information, that is *forgery*, *impersonation*, *in-transit traffic tampering* and *on-board tampering*.

Infotainment: These applications are vulnerable to behaviors that are associated with transmission of false information and violation of personal user data. Therefore, *forgery* and *privacy violation* are more likely to cause problems in infotainment applications.

REFERENCES

[1] A. Caragliu, C. Del Bo, and P. Nijkamp, “Smart cities in Europe,” *Series Research Memoranda 0048*, 2009.
[2] S. Mathur, T. Jin, N. Kasturirangan, J. Chandrasekaran, W. Xue, M. Gruteser, and W. Trappe, “Parknet: Drive-by sensing of road-side parking statistics,” in *Proc. 8th ACM MobiSys*, San Fran., USA, 2010.
[3] SFpark: parking system for San Francisco, available online in http://sfpark.org/.
[4] Parking Defenders mobile application, available online in http://www.parkingd.com.
[5] Parkomotivo: parking system for the city of Lugano, available online in http://www.bmob-park.
[6] http://www-03.ibm.com/press/us/en/pressrelease/35515.wss.
[7] H. Wang and W. He, “A reservation-based smart parking system,” in *Proc. 5th Inter. Workshop on Cyber-Physical Networking Systems (colocated with IEEE INFOCOM)*, April 2011.
[8] M. Caliskan, D. Graupner, and M. Mauve, “Decentralized discovery of free parking places,” in *Proc. 3rd VANET (in conjunction with ACM MobiCom)*, USA, 2006.
[9] E. Kokolaki, M. Karaliopoulos, and I. Stavrakakis, “Opportunistically assisted parking service discovery: Now it helps, now it does not,” *Pervasive and Mobile Computing*, vol. 8, no. 2, 2012.
[10] T. G. Kurtz, “Solutions of ordinary differential equations as limits of pure jump Markov processes,” *Journal of Applied Probability*, 1970.
[11] M. Gerla and L. Kleinrock, “Vehicular networks and the future of the mobile internet,” *Computer Networks*, vol. 55, no. 2, 2011.
[12] M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications,” *IEEE Wireless Communications*, 2006.
[13] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Workshop on the Hot Topics in Networks (HOTNETS-IV)*, 2005.
[14] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *J. Comput. Secur.*, vol. 15, no. 1, 2007.
[15] B. Aslam and C. Zou, “Distributed certificate and application architecture for Vanets,” in *Proc. 28th IEEE MILCOM*, Piscataway, USA, 2009.
[16] V. Verroios, V. Efstathiou, and A. Delis, “Reaching available public parking spaces in urban environments using ad hoc networking,” in *Proc. 12th IEEE MDM*, Beijing, China, 2011.
[17] T. Delot, N. Cenerario, S. Ilarri, and S. Lecomte, “A cooperative reservation protocol for parking spaces in vehicular ad hoc networks,” in *Proc. 6th Inter. Conference on Mobile Technology, Application and Systems*, ser. MOBILITY, 2009.