Analysis of Inter-RSU Beaconing Interference in VANETs

Carlos Gañán[1], Jonathan Loo[2], Jose L. Muñoz[1], Oscar Esparza[1]
Sergi Reñe[1] and Arindam Ghosh[2]

[1]Universitat Politècnica de Catalunya, Telematics Department, Barcelona (Spain) **
{carlos.ganan,jose.munoz,oscar.esparza,sergi.rene}@entel.upc.edu
[2]Middlesex University, Computer Communication Department, London (UK)
{j.loo,a.ghosh}@mdx.ac.uk

Abstract. Vehicular ad Hoc Networks (VANETs) have emerged as a key technology serving community of peoples in various applications. Providing infotainment and safety services requires the existence of road-side units (RSU) to access to the desired resources. Ideally, the infrastructure should be deployed permeatively to provide continuous connectivity and optimal coverage. This deployment technique increases capacity and coverage at expenses of increasing interference that can severely degrade the performance of the VANET. Moreover, malicious vehicles could mimic the signals of RSUs causing significant performance degradation. In this paper we study the impact of the inter-RSU interference on the beacon broadcasting due to both inefficient deployment and potential RSU emulation attacks (REA). Extensive packet-level simulations have been performed to support the observations made.

Keywords: VANET, RSU interference, RSU emulation attack.

1 Introduction

Vehicular ad hoc networks (VANET) will be deployed around the world within the next years. Covering a very dense environment requires that thousands of road side units have to be placed and set up properly, without interference. Thus, a main requirement of an efficient VANET is adequate coverage where vehicles are able to access (e.g., pervasive computing-enabled) applications and services. The deployment of the infrastructure should reduce the interference as much as possible so as to achieve these functions in a cost-effective and resource-efficient manner.

** This work is funded by the Spanish Ministry of Science and Education under the projects CONSOLIDER-ARES (CSD2007-00004), FPU grant AP2010-0244, and TEC2011-26452 "SERVET", and by the Government of Catalonia under grant 2009 SGR 1362.

Regrettably, RSUs will be deployed in an empirical way, manually positioned and located based on the received signal strength. Such an unorganized approach to VANET infrastructure design implies strong channel interference and poor resource utilization. For instance, more RSUs may be used to improve coverage while leaving blind spots or places where there are too many RSUs packed too closely together. This will lead to signal overlap, which in turn will cause interference and waste of resources. In this paper, we address to quantify the impact of this interference on the VANET performance.

The medium access control (MAC) for Wireless Access in Vehicular Environments (WAVE) described in the IEEE 1609.4[1] is unable to cope with the sharp increase in interference caused by these dense deployments. Moreover, most of the applications envisioned for this type of networks require the periodic broadcasting of beacons and WAVE service advertisement (WSA). Beacons are generated with typical frequency of 1-10 Hz; this high generation rate could cause not only the congestion on the control channel (CCH) but also the loss of beacons containing critical information. Moreover, the current standard do not provide any authentication mechanism for the CCH. An adversary equipped with a software defined radio can mimic the transmission characteristics of a RSU in order to emulate its activity. The goal of this attack is to block vehicles from utilizing the idle service channels, thus reducing the available bandwidth and degrading the network performance. The malicious attackers can thus significantly degrade the performances of the well-behaving vehicles by causing additional collisions in the CCH and reserving service channels for their own benefit.

Broadcasting in VANETs has been studied from the vehicle to vehicle (V2V) point of view [2, 3], however the role of the RSUs has been neglected. Authors have modeled analytically broadcast transmissions even taking into account he channel switching [4], but only from a V2V perspective. WAVE services will be announced by the infrastructure during the CCH. Though these advertisements will not be as delay-constraint as the safety applications, it is necessary to provide a reliable broadcasting service via RSUs. The lack of an authentication mechanism introduces an entire new suite of threats and tactics that cannot be easily mitigated. RSU emulation attacks (REA) can be easily performed by any malicious vehicle by broadcasting nonexisting or fraudulent WSAs.

In this paper we analyze the unreliable broadcast service from the infrastructure perspective. We show that one of the main issues for broadcast protocols lies in the unreliable packet delivery. While the IEEE 1609.4

uses RTS/CTS handshake mechanism for unicast transmissions to increase reliability, beacons will be broadcasted in the CCH relying only on pure CSMA/CA without RTS/CTS. By means of realistic simulation we show the inability of the broadcasting mechanism to achieve a beacon reception rate close to 100%. Just introducing a single attacker performing a RSU emulation attack could lead to a beacon collision probability above the 35%. We show that this problem is especially critical in VANETs where safety beacons will collide and will not be received in time to prevent accidents.

2 IEEE 1609.4 Broadcasting Limitations

Vehicular denseness will vary from very dense urban areas to sparse highways. Therefore, the MAC layer of the VANET has to be scalable. The IEEE 1609.4 [1] is based on the Distributed Coordination Function (DCF) as MAC technique. DCF employs a CSMA/CA with binary exponential backoff algorithm. This mechanism is enhanced by using the same prioritization techniques than the IEEE 802.11e [5], namely the Hybrid Coordination Function (HCF). Basically, the HCF allows making Arbitration Interframe Space (e.g. AIFS[i]) variable depending on the priority (i) of the packet (see Fig. 1). Also, the length of the contention window varies among different priorities.

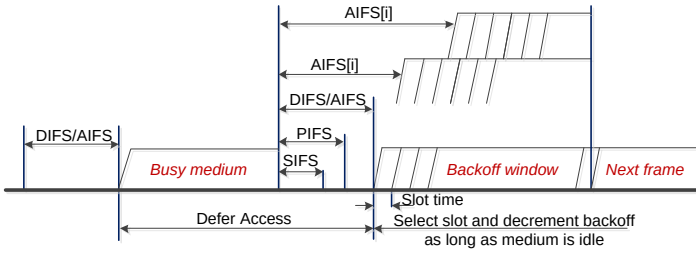


Fig. 1. EDCA channel access prioritization, as specified in [5]

However this MAC mechanism is neither secure nor efficient for dense networks. The CSMA/CA does not totally avoid collisions when broadcasting. Similar to the traditional unicast IEEE 802.11, it presents drastic throughput falls in crowded environments. Moreover, for broadcast communication, there is no error-handling as there are no acknowledgments and hence no exponential backoff growth. In this sense, as the

contention window size is not increased, the prioritization is limited and even increases the likeliness of packet collisions. Broadcast beacons suffer from hidden node problems, due to the lack of a RTS/CTS handshake. Moreover, safety beacons are sent with the maximum transmission power, which increased the coverage and, consequently, the inter-RSU interference. According to the different signal strengths, we can distinguish three different ranges (see Figure 2):

- *Communication range*: is the region where both the vehicle's receiver sensitivity threshold and the SINR are met for the payload.
- *Detection range*: is the region where other vehicles can detect an ongoing transmission.
- *Interference range*: is the region starting from the precise location where there is not enough signal power to decode the packet.

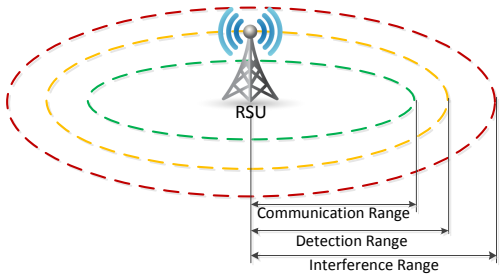


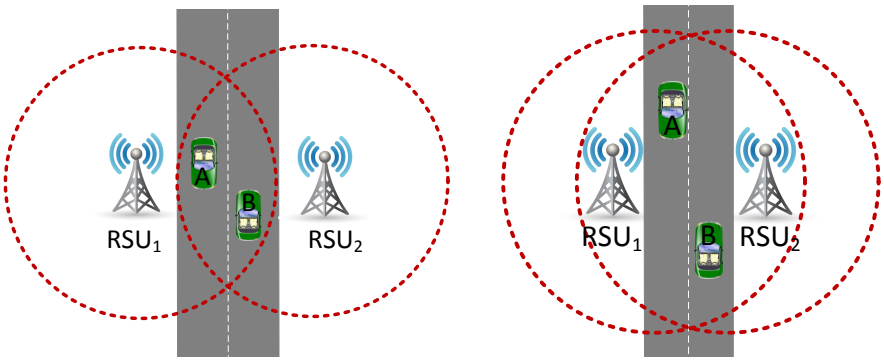
Fig. 2. Transmitting-RSU ranges.

Thus, when broadcasting the MAC mechanism described in the IEEE 1609.4 standard will incur in high delays due to channel switching and will suffer from the hidden problem which will lead to beacon collisions. Moreover, as these beacons are not authenticated, any entity with a 802.11p interface could emulate a RSU and broadcast beacons leading to denial of service. Current IEEE 1609.4 cannot cope with these attacks which could lead to a severe degradation of the network performance.

3 Inter-RSU interference

In this section, the interference between several RSUs is analyzed. Different interference scenarios are distinguished according to the distance, D, between the RSU. These scenarios will appear either to an inefficient

RSU deployment or to the existence of attacker performing REA attacks. In this paper, we only take into account the interference from within the communication range of the RSUs. A RSU is said to be interfered by another RSU if the vehicles in its transmission range are able to decode the packets from the interfering RSU.



(a) Type-A ($R < D \leq 2R$) (b) Type-B ($D \leq R$)

Fig. 3. Inter-RSU interference scenarios.

Fig. 3 shows two different inter-RSU interference scenarios, i.e., Type-A and Type-B interference scenarios correspond to $R < D \leq 2R$ and $D \leq R$, respectively, where R is the communication range. Note that for larger distances, there is no interference between both RSUs. Before delving further into the characteristics of each interference scenario, we define the overlapping region O as the intersection region of the transmission range of the RSUs.

In Type-A scenarios, RSUs are not within communication range of each other and this cannot decode each other's transmitted beacons. Although the RSUs can hear from the vehicles of the interfering RSU, the interfering RSU and the vehicles in its range can become hidden nodes. For instance, as in Fig. 3(a), when RSU_1 and RSU_2 are broadcasting beacons, these beacons could potentially collide as both RSUs are hidden nodes one to the other. Thus, both vehicles in region O will suffer from beacon losses. Therefore, the beacon transmission from RSU_1 is not successful at vehicle A due to a colliding transmission from RSU_2. Traditionally this problem is addressed by the RTS/CTS/DATA/ACK handshake. However, when broadcasting the IEEE 1609.4 standard does

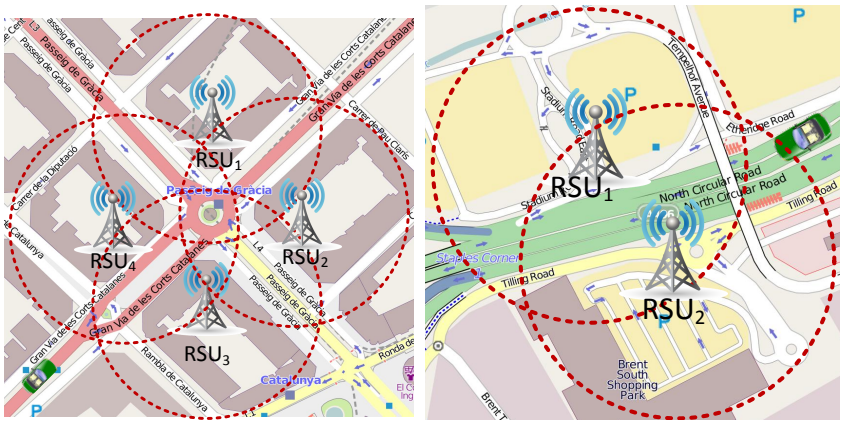
not use this handshake. Therefore, the hidden RSU effect will be one of the main reasons for packet loss in vehicular communication.

For Type-B (see Fig. 3(b)), a RSU can receive direct transmissions from the interfering RSU and some or all of the vehicles in its range. The problem faced by Type-B interference scenario is that all the entities in the transmission range of either one of the RSUs (i.e. vehicles or the interfering RSU) can become potential hidden nodes to the ongoing transmission. As RTS/CTS is not used when broadcasting, vehicles may be exposed to a beacon drop in the message queue in high load scenarios where the carrier is nearly all the time found busy. The connection to packet loss here is that for the exposed RSUs the local message queue becomes full. In the worst case, not even one beacon can be sent. Such a situation can be described as local beacon congestion. Beacon loss then occurs depending on the packet dropping strategy. If we now consider highly varying RSU densities this consideration also reveals that even in locally low densities RSUs may be exposed if there are high densities within carrier sensing range. In this case, some RSUs would be blocked from transmission unnecessarily. Therefore, in both type of interference scenarios, it is clear that a significant number of beacon collisions will occur when broadcasting.

4 Evaluation

In this section, extensive packet-level simulations are performed to validate the observations made in the previous section. We use the VeinS simulator to evaluate the impact of the inter-RSU interference. VeinS [6] is an inter-vehicular communication simulation framework that integrates the OMNeT++/ INET [7] network simulator and the SUMO [8] road traffic microsimulation tool. VeinS implements a multi-channel simulation model for IEEE 1609.4/802.11p allowing to fully capture the distinctive properties of this radio technology.

We use two real scenarios (each one representing a different interference Type) to evaluate the inter-RSU interference (see Fig. 4). First, we evaluate a urban intersection of the Spanish city of Barcelona. According to the Spanish transport authority, annually, in Barcelona from 70 to 100 intersections are detected with more than ten accidents, with a total of 1,500 accidents, near 60% of those produced in the entire city. Typically, these accidents are concentrated at intersections of roads with two lanes. The second scenario is a urban motorway located in the city of London. Due to the high density of cars and roads in this area, it is foreseeable



(a) Urban Intersection (Type-A) (b) Motorway (Type-B)

Fig. 4. Simulation scenarios.

that the RSU will overlap as in a Type-B interference scenario. The configuration parameters of the RSUs/vehicles are shown in Table 4. Note that cars are placed in each scenario moving across the intersection in the Type-A scenario and moving through the motorway in the Type-B scenario. Each RSU broadcast beacons in the CCH with the highest priority. SUMO [8] is used to recreate a realistic traffic environment.

Parameter	Value
Transmission Power	20 mW
Bit rate	18 Mbps
Sensitivity	-94.0 dBm
Thermal Noise	-110.0 dBm

Table 1. RSU configuration parameters.

Parameter	Value
Speed	20 m/s
Max. Acceleration	5 m/s
Max. Deceleration	3 m/s
Channel bandwidth	10 MHz
OBU receiver sensitivity	-94.0dBm

Table 2. Vehicle profile.

4.1 Performance Metrics

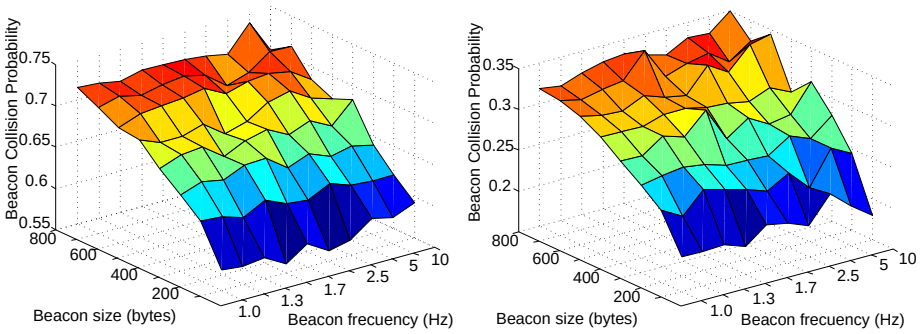
We define four different metrics to evaluate the inter-RSU interference:

- *Beacon Collision Probability* (P_{col}): probability that a beacon broadcasted by RSU_j collides with another beacon broadcasted by RSU_i.
- *Delay*: elapsed time since the creation of the beacon from RSU_j and the reception at vehicle_i. This is only calculated for received beacons.

– *Per-vehicle Throughput* (T): size of the beacons delivered to a particular vehicle over a period of time.
– *Inter-arrival Time* (τ): amount of time between two successive beacon receptions at vehicle$_i$. This is important from the point of view of a real-time applications. Ideally, the inter-arrival time would equal the beacon generation interval.

4.2 Simulation Results

Beacon Collision Probability Fig. 5 shows P_{col} for different beacon sizes (b_s) ranging from 100 to 800 bytes, and different beacon generation frequencies (BGF) raging from 1 to 10 Hz. As expected, the collision probability increases with both b_s and BGF. It is worth noting that P_{col} is higher in the Type-A scenario as all the RSUs are hidden one to each other. Thus, the collision avoidance mechanism is totally inefficient, and P_{col} achieves values higher than the 70%. In the Type-B scenario, the hidden terminal problem is not that frequent. Therefore, the collision probability is lower.



(a) Type-A (b) Type-B

Fig. 5. Beacon Collision Probability P_{col}.

The scenario with $b_s = 800$ bytes and BGF = 10Hz is shown in Fig. 6. In this case, it is clear than when a vehicle is in range of 4 RSUs, the number of collision highly increases. In the London motorway, the CSMA/CA avoids most of the collisions but it is not able to avoid that some of the beacons collide.

The required reception probability depends on the type of application supported by the vehicular network. However, for safety application P_{col}

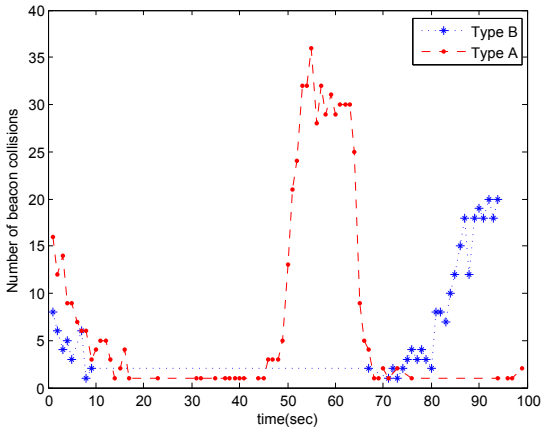
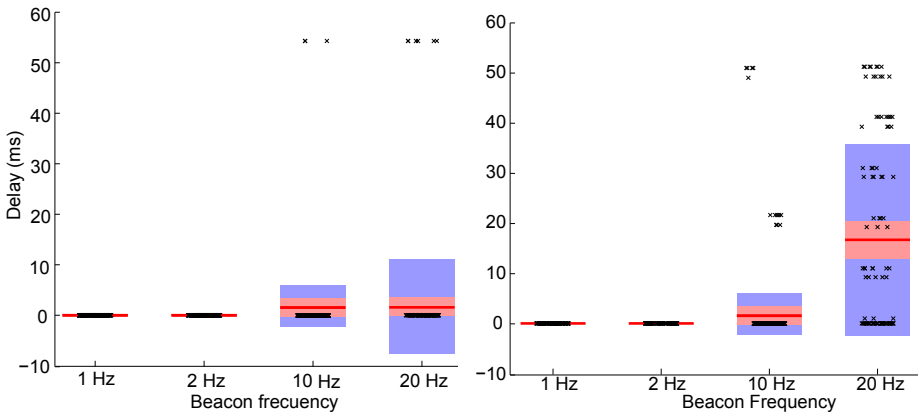


Fig. 6. Number of beacon collisions for b_s= 800 bytes and BGF=10 Hz

should not exceed the 1%. As shown this requirement not met when the vehicle is in range of two or more hidden RSUs. The simulation results show that a P_{col} below 1% is only achieved in Type-B scenarios when the BGF is under 10Hz and the beacon are smaller than 200 bytes.

Delay Analysis We furthermore analyzed the beacon delay, i.e., the time from the generation of a beacon message at the RSU to its actual reception at the vehicle under different BGF. We visualized our findings in Fig. 7. As shown in Fig. 7, while for low frequencies (BGI< 10 Hz) the differences between Type-A and Type-B scenarios are very small. Significant differences appear when the BGF> 10Hz. This is due to the impossibility to distribute the beacons over only Control Channel intervals. With this BGF, all beacons generated during a Service Channel interval have to wait for the next CCH interval to be sent. Therefore, a beacon has to wait at most of 54 ms until it is sent. Note also, that for BGF> 10 Hz the delay is higher in the Type-B scenario. The reason for that is that in Type-B when a RSU detects that the channel is busy it enters into a back-off interval.

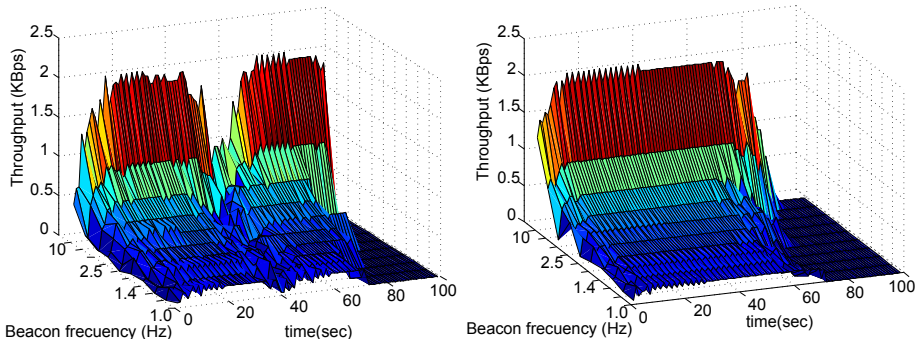
Per-vehicle Throughput Fig. 8 shows the impact of the BGF on per-vehicle throughput. As expected, when beacons are generated more frequently, the throughput increases. However, this increment is not directly proportional to the BGF as there are more collisions when BGF increases. Note that, while in the Type-B scenario the throughput remains roughly



(a) Type-A (b) Type-B

Fig. 7. Delay Box-Plot for b_s= 800 bytes.

constant during the simulation time, in the Type-A scenario the throughput varies over time.



(a) Type-A (b) Type-B

Fig. 8. Throughput evolution vs BGF

.

Fig. 9 shows the throughput for b_s= 800 bytes and BGF=10Hz. Note that in the case of the Type-A scenario, when the vehicle is in range of the four RSUs, the throughput decreases drastically. This is due to the high number of collisions. After 40s, the vehicle is at the intersection and the 4 RSUs are broadcasting beacons as if the medium was idle. Thus, almost all the beacons collide (see Fig. 6) and the throughput drops to almost 0 KBps.

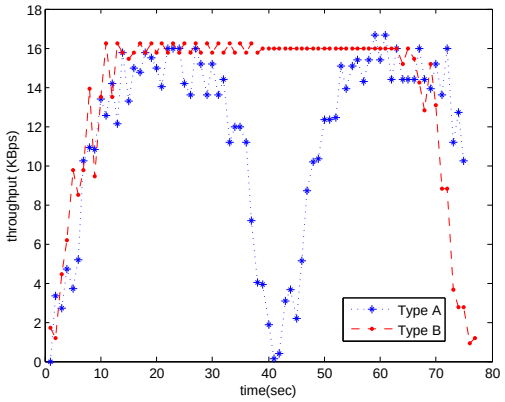
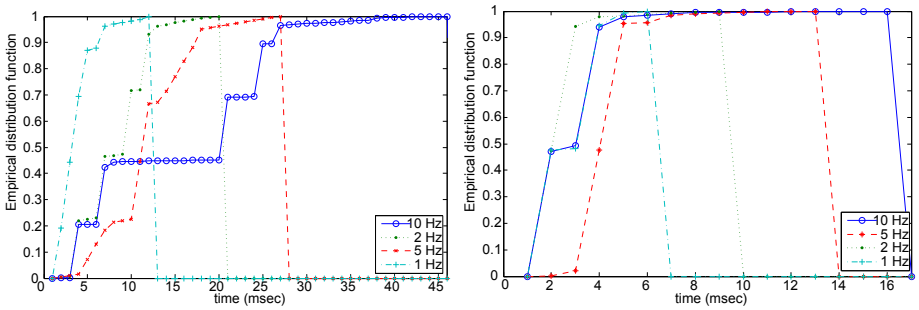


Fig. 9. Throughput for b_s= 800 bytes and BGF 10 Hz

Inter-arrival Time Fig. 9 shows the empirical cumulative distribution function (ECDF) of τ for different BGF. As the BGF increases P_{col} increases, with a detrimental effect on the inter-arrival time of beacons. Thus, τ increases for larger BGF values. This is a direct consequence of the beacon collisions. When a RSU transmits a beacon and this beacon is lost, it is not retransmitted. At the next beacon issuing instant, the RSU will transmit a new beacon with updated information. This effect is more evident in Type-A as there are more collisions. Due to this periodicity, the ECDF of τ adopts a staircase shape. In the Type-B scenario, τ is lower (as there are fewer collisions).



(a) Type-A (b) Type-B

Fig. 10. ECDF of Inter-arrival times for b_s = 800 bytes.

5 Conclusions

In this paper, we have shown that inter-RSU interference will appear due to either inefficient RSU deployment or the existence of RSU emulation attacks. We have shown that current IEEE 1609.4 medium access technique is not able to cope with the interference caused by overlapping RSUs. The analysis of the beacon collision probability shows that the broadcast performance drops below 30% when a vehicle is in range of four RSUs that are hidden one to the other. Moreover, due to the channel switching scheme defined in the IEEE 1609.4, the delay can exceed the 54 ms, making unfeasible the deployment of a safety applications.

The insights gained from this analysis not only lead to a better understanding of the impact of inter-RSU interference on VANETS but also can be used to design improved beaconing techniques to mitigate the RSU emulation attacks.. Future work includes identifying REA attackers and exclude them from the network.

References

1. IEEE draft standard for wireless access in vehicular environments (WAVE) - multichannel operation. *IEEE 1609.4/D8.0*, pages 1 –92, June 2010.
2. Alexey Vinel, Yevgeni Koucheryavy, Sergey Andreev, and Dirk Staehle. Estimation of a successful beacon reception probability in vehicular ad-hoc networks. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC '09, pages 416–420, 2009.
3. C. Campolo and A. Molinaro. On vehicle-to-roadside communications in 802.11p/wave vanets. In *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, pages 1010 –1015, march 2011.
4. C. Campolo, Y. Koucheryavy, A. Molinaro, and A. Vinel. Characterizing broadcast packet losses in ieee 802.11p/wave vehicular networks. In *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, pages 735 –739, sept. 2011.
5. IEEE Standard for Information Technology - Telecommunications and Information Exchange between systems - local and metropolitan area networks - specific requirements. *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11)*, pages 1 –189, November 2005.
6. C. Sommer, R. German, and F. Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *Mobile Computing, IEEE Transactions on*, 10(1):3 –15, jan. 2011.
7. A. Vargas. Objective modular network testbed in c++ (omnet++). version 4.2. Available: www.omnetpp.org.
8. D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner. SUMO (simulation of urban mobility); an open-source traffic simulation. In *4th Middle East Symposium on Simulation and Modelling (MESM2002)*, MESM2002, pages 183–187, 2002.