Beaconing in a Highway Scenario: Vulnerable Vehicles Problem

Ali Bin Tariq
Department of Communications Engineering
Tampere University of Technology, Finland
alibtariq@gmail.com

Abstract

Periodic exchange of short status messages using IEEE 802.11p also referred to as beaconing is a core inter-vehicle communication mode enabling novel cooperative safety applications. A beaconing in the platoon of vehicles moving on a highway is studied as one of the popular practical scenarios. This paper demonstrates that when the inter-arrival times of beacons are small and under certain medium access control protocol parameters, some vehicles in the platoon may suffer from serious performance degradation. The condition when such situation takes place is studied and recommendations are given on a proper choice of IEEE 802.11p parameters.

Index Terms: Beaconing, Hidden-nodes, IEEE 802.11p, VANET.

I. Introduction

In recent years vehicular ad-hoc networks (VANETs) are attracting a lot of research interest from academia as well as automotive industry. The availability of IEEE 802.11p wireless interface and a provision of wireless communication among vehicles can significantly enhance the traffic safety and subsequently add some important features in the vehicular experience. There are wide varieties of applications that can be supported in VANET-based system, but most importantly the need of VANET arises when it comes to the safety and traffic monitoring. Such kinds of applications include information about emergency alerts, unpredicted road conditions, sudden change of a driving lane, hazard and emergency warning systems, collision avoidance, intersection coordination, driver assistance system and traffic sign or signal violation, etc. Apart from the safety applications VANETs can offer several other features such as availability of digital maps, multimedia applications and gaming, etc.

There are two kinds of messages used by the safety applications: they are generated to provide precise and latest status and hazard information to the driver. They are termed as event-driven (DENMs – Decentralized Environmental Notification Messages) and periodic messages (CAMs – Cooperative Awareness Messages). Event- driven messages are only generated when an actual accident has occurred or a hazard has been detected, while the periodic messages, which are also known as beacons, are generated continuously to inform the neighboring vehicles about their status. Typical beacon contains vehicle‘s position, speed, direction, etc. Beacons are used to keep all the vehicles, in the same geographic area, constantly updated about the surrounding. Beacons are normally transmitted using the IEEE 802.11p carrier-sense random multiple access approach with the rates of 1-10 Hz. The corresponding multiple access channel load is determined by the density of nodes. Beaconing is a key communication mode in VANETs and is a subject to intensive research at the moment [1].

In [2] the problem of the channel congestion and the corresponding choice of a beacon generation rate basing on the vehicles movement patterns is studied. Similarly the effect of beaconing is studied in [3] using the concept of tracking accuracy. In this paper a control of the beaconing rate and transmission power is introduced to avoid channel congestion and at the same time to achieve a minimum acceptable tracking accuracy of the neighboring vehicles. Both of the above references use the highway scenario, which is also modeled in this study.

Some of other relevant studies about the beaconing are preformed in [4], [5] and [6]. The authors of [4] studied the effect of contention window on the performance of beaconing in VANET by means of simulations. They showed that increasing the contention window in a dense traffic environment will result in an improved beacon performance in terms of successful reception probability. Similar observations are done in study [5], where it is demonstrated by means of a stochastic modeling that in a highly dense traffic environment the beacon reception probability for standardized parameters can become unacceptably low; while it typically satisfies the delay requirements. Paper [6] suggests a one-hop broadcast protocol, in which the probability of successful reception for beaconing is increased by adaptively controlling the transmission power and adjusting the contention window size.

The hidden node problems in VANETs make it difficult to provide a reliable communication between the nodes. In a typical hidden node scenario, two nodes which are not interfering with each other share a set of nodes which are in the communication range of both of the nodes thus resulting in a corrupted reception at the shared node. Hidden node problem and its solutions have been widely studied, e.g. in [7] for the unicast traffic in 802.11 and the RTS/CTS (request-to-send/clear-to-send) approach. However, due to the broadcast nature of the beaconing in vehicular networks and unavailability of any MAC-layer acknowledgement or retransmission techniques, this problem differently influences the performance of VANETs. In this paper, the typical “highway” scenario is focused, when vehicles are assumed to be located on the line. It has been demonstrated that poor selection of MAC parameters can degrade the performance of some particular nodes in the highway scenario. These degraded nodes are referred as “vulnerable” nodes. In comparison to traditional approach when probability of successful beacon delivery is derived for the overall VANET, it has been demonstrated that this value is significantly different for different nodes. Therefore, the existence of “vulnerable” nodes may lead to impossibility of implementing cooperative safety applications based on beaconing, although the network-wide averaged values of performance metrics might look reasonable.

The paper is organized as follows. Section I deals with the introduction, concept of safety messages in VANET, related research and a brief description of the problem studied in this research. In Section II we present the system model and the assumptions on which the model is based. Section III is distributed in two subsections: in part A simulations are carried out with two different sets of parameters (ideal and realistic) and the effect of fairness is studied while in part B an analytical study of the problem is discussed. Section IV is conclusion and provides recommendation on the suitable usage of MAC parameters.

II. System Model

In this simplistic model communication between the nodes in vehicular network operating according to the IEEE 802.11p is discussed. Basic assumptions of this model are summarized below:

1. A platoon of N vehicles located on the line is considered; inter-vehicle distance is fixed and is taken as unit of length;
2. Topology of the network is assumed to be fixed during the overall system operation;
3. Each node communication range is limited to d=1 (both in forward and backward directions); the carrier sense range coincides with the communication range;
4. The radio channel is ideal, so bit errors are not considered;
5. All nodes broadcast the beacons of L [bits] with data rate R [bits/sec]; T_h is the duration of Physical Layer Convergence Protocol (PLCP) preamble and header used for each beacon;
6. Nodes operate independently of each other according to IEEE 802.11p and have their own “picture” of the events occurring in the channel; possible channel events are success, collision and empty; IEEE 802.11p MAC parameters W (contention window) and interframe spaces (AIFS and EIFS) are given;
7. All nodes always have packets ready to send (saturation conditions).

The assumptions above are motivated mostly by the cooperative adaptive cruise control (CACC) application, where vehicles in the platoon strive to maintain a constant speed as specified by the lead vehicle [8]. Initial experiments with CACC use the connection only between the neighboring vehicles in the platoon that justifies the assumption (iii). The simulations are carried out with the assumption of a saturated network (vii), however, in reality the frequency of 10 Hz is used. In a typical VANET-based system, vehicles may not always have packet ready to be transmitted but this assumption allows modeling the worst case scenario. Moreover, it is not yet completely clear whether higher than 10 Hz beaconing rates are needed for CACC or not, e.g. for high speeds.

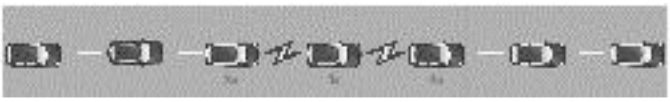

Fig. 1. Vehicles Uniformly Distributed on the Highway

III. Vulnerable Vehicles Problem

A. Simulation Results

In this study we have evaluated the impact of inter-arrival times of beacon under certain MAC parameters. It is observed that the size of contention window and EIFS are pivotal in determining the fairness of the system. The fairness is analyzed by counting the number of transmission attempts, a particular node has made during the simulation run or in other words the periodicity by which the node has tried to access the channel. Initially the fairness test is run with the simplistic of parameters as shown in Table 1. The duration of successful transmission is $T_s=T_h+L/R+AIFS$, whereas duration of corrupted transmission is given as $T_c=T_h+L/R+EIFS$. In terms of slot time the length of successful and collided transmission is $s=T_s/\sigma$ and $c=T_c/\sigma$.

TABLE I
IDEAL (SIMPLISTIC) SIMULATION PARAMETERS

Parameter	Value
Nodes	20
W	4
aifs	1
eifs	1
t	1
Simulation Time(slots)	10^5

Two simulation runs were carried out to count the total number of transmission attempts by an individual node. Following is the results that are yield from the two simulations run with the same parameters.

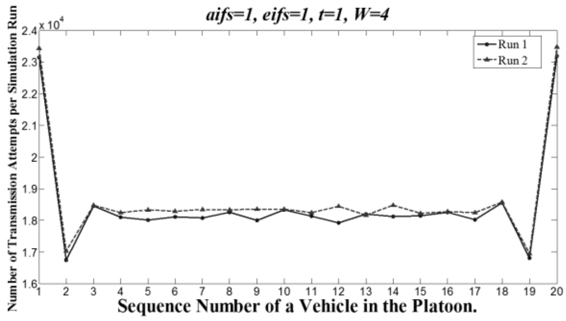

Fig. 2. Fairness Check (Ideal Parameters)

As it is evident from Fig 2, all the vehicles in the platoon have recorded almost same number of transmission attempts except the first and the last node. The reason for this increase is due to the fact that this model depicts a highway scenario that is replicated as a straight line, so the first and last node can receive packet from only one direction; thus have less chances of direct collision (two neighboring nodes transmitting simultaneously), less probability of becoming hidden nodes and ultimately have more chances of transmission. For precisely the same reason the second and the second-last node are suffering from a bit of starvation because most of the time their neighboring nodes are transmitting beacons and these particular nodes do not have enough opportunities to transmit their beacons. By taking this test one step further, the fairness is check with real parameters for different contention window sizes. Ideal parameters are given in table 2. IEEE 802.11p draft PHY-layer constants are taken from [9].

TABLE II
REALISTIC SIMULATION PARAMETERS

Parameter	Value
σ	16 µs
Nodes	20
W	[4,32,128]
EIFS(*eifs*=EIFS/ σ)	188µs (188µs/16≈12)
AIFS(aifs=AIFS/ σ)	64µs (64 µs/16=4)
L	500 Bytes
R	3 Mbps
Header duration(T_h)	40 µs
Transmission Time of Packet ($t \approx (T_h+L/R)/\sigma$)	83 (slot time)
Simulation Time(slots)	10^5

Through the simulation it is observed that an increase in the interframe space with a varying contention window will have an adverse effect on the fairness of the system. This degradation of performance is shown in Fig. 3.

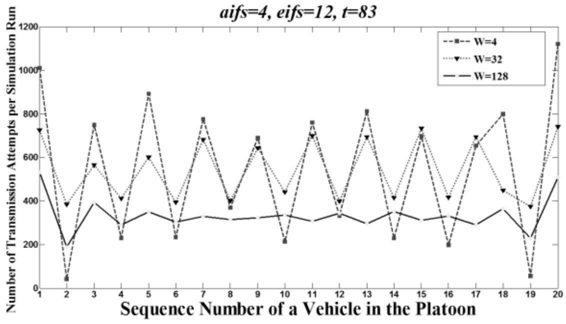

Fig. 3. Fairness Check (Realistic Parameters)

Fig. 3 illustrate three graph representing number of transmission attempts made by individual nodes in the platoon for different contention window sizes. As it can be seen from the figure that for *W*=128 the fairness is achieved and the result is quite similar as with the ideal parameters (Fig 2) but for *W*=4 and *W*=32 there is severe degradation in performance and fairness is not guaranteed. The reasons for such a discrepancy for lower contention window size is due to the difference in the size of contention window and combine size of *EIFS* and *L*. When the node is waiting for *EIFS* after a collision, it is quite possible that its neighboring node will start to transmit again since the difference in the size of contention window and the combine size of *EIFS* and *L* is not large enough, so there is a chance that a node during the whole simulation run will not get enough opportunities to transmit the packet and thus suffer from starvation.

Another figure of merit to study the performance degradation is the contention delay. Studies [4;5] have concluded that it is easy to meet the delay requirement in a beaconing scenario and because of the importance of beaconing for a safety scenario the general rule of thumb is also to have less contention delay while broadcasting beacons.Through the simulation tests, it is observed that lower contention window guarantees a minimum delay but, due to the starvation, the contention time is significantly high as shown in fig 4.

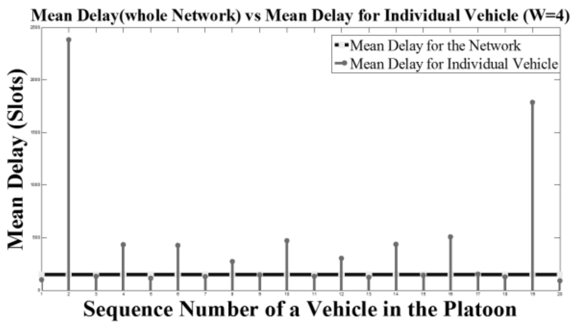

Fig. 4. Contention Delay

This performance degradation and vulnerability of a vehicle is further explained in the timeline presented in Fig. 5. Consider a CACC system consisting of 3 nodes operating according to IEEE 802.11p standard. Initially backoff counter of node 1 expire which results in beacon transmission to node 2. In the meanwhile backoff counter of node 3 also expire which results in transmission of beacons from node 3 to node 2. Consequently there is a packet collision at node 2 because beacons from node 1 and node 3 are now collided at node 2 (hidden node scenario). Subsequently node 2 will wait for EIFS and the corresponding backoff time before contending for the channel access, at this instance node 1 after finishing its transmission and waiting time (AIFS) is waiting for gaining access to the channel and since the size of contention window is small so there exists a possibility that node 1 will transmit a beacon way before node 2 finishes its waiting time (EIFS). Thus limiting the opportunity of node 2 to transmit and subsequently transmission from node 3 can cause a packet collision at node 2 as explained previously (node 2 is receiving beacons from node 1 and node 3, refer to Fig 5). In this way Node 2 will suffer from severe performance degradation and thus become vulnerable.

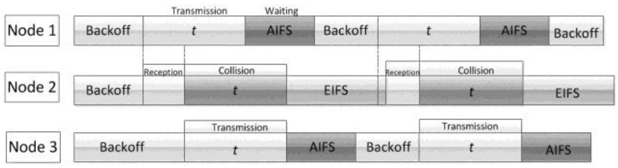

Fig. 5. Vulnerable Node

B. Analytical Results

With reference to the timeline presented in Fig. 5, an analytical explanation of the vulnerability of vehicles is presented in this section. Please note that this behavior (vulnerability of nodes) is observed for low contention window sizes. For simplicity, the number of vehicles contending for channel access is restricted to 3. Two cases are considered for analytical study i) Node 1 and Node 3 are synchronized, meaning that both nodes will finish their backoff counter at the same time. Though in reality the possibility of a synchronized node 1 and node 3 are minute but through this assumption we can study the effect of some of the MAC parameters. ii) Node 1 and Node 3 are not synchronized as in most realistic cases.

A case for synchronized node 1 and node 3 is shown in figure 6; in that case if the duration of *EIFS* at node 2 is greater than the combine durations of *AIFS* and maximum value of backoff counter for both the node 1 and node 3, it implies that node 2 will always be killed after the first collision.

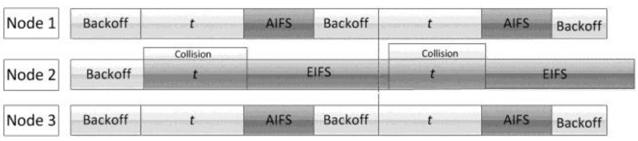

Fig. 6. Vulnerable Node (Synchronous Case)

Mathematically it can be written as,

$$EIFS > AIFS + (W-1)\sigma$$

$(W-1)\sigma$ represents the maximum value of the backoff counter for node 1 and node 3. If the above condition holds true, node 2 will suffer from serious starvation and will not have enough opportunities to transmit the packet and consequently affect the overall performance of the system.

Similarly a case for an asynchronous node 1 and node 3 is shown in figure 7; it is a replica of Fig. 5. In this case after the first collision at node 2, node 2 will suffer from starvation if the combine duration of the transmission time of packet*(t)* and *EIFS* is greater than the sum of maximum backoff counter value and *AIFS.*

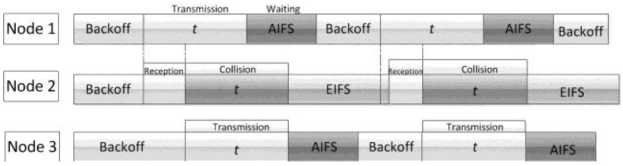

Fig. 7. Vulnerable Node (Asynchronous Case)

Mathematically,

$$t\sigma+EIFS>AIFS+(W-1)\sigma$$

As mentioned previously $(W-1)\sigma$ represent the maximum value of backoff counter. Thus for low contention window sizes, having a large duration of *t* and EIFS means a starved node 2 as shown in figure 7. The above equation (asynchronous case) can alternatively be written as

$$t+eifs>aifs+(W-1)$$

It implies

$$W>t+eif-aifs+1$$

If the above equation holds true then the chances of node starvation is minimum and the system will have a relative fairness or alternatively the above equation indicates the scenario when all the nodes will make somewhat equal number of transmission attempts and the performance of the system will not be degraded and thus the effect of the vulnerable nodes will be minimal.

REFERENCES

[1] VANET - Vehicular Applications and Inter-Networking Technologies, (Editors: Hannes Hartenstein, Kenneth Laberteaux), John Wiley & Sons, ISBN: 978-0-470-74056-9, 472 pages, Jan. 2010.
[2] Schmidt R., Leinmuller T., Schoch E., Kargl F. and Schafer, G.,"Exploration of Adaptive Beaconing for Efficient Intervehicle SafetyCommunication," IEEE Network, Vol. 24, No. 1, pp.14-19. Jan-Feb 2010.
[3] C.-L. Huang, Y. Fallah, R. Sengupta, andH. Krishnan, "Adaptive IntervehicleCommunication Control For CooperativeSafety Systems", IEEE Network,Vol. 24, No. 1, pp. 6–13, Jan-Feb. 2010.
[4] Reinders, R.; van Eenennaam, M.; Karagiannis, G.; Heijenk, G.; , "Contention Window Analysis For Beaconing In Vanets," Proceedings of 7thInternationalWireless Communications and Mobile Computing Conference (IWCMC-2011) Istanbul, Turkey,pp.1481-1487, 5-8 July 2011.
[5] A. Vinel, Y. Koucheryavy, S. Andreev, and D. Staehle, "Estimation Of A Successful Beacon Reception Probability In Vehicular Ad-Hoc Networks,"Proceedings of 5th International Wireless Communications and Mobile Computing Conference (IWCMC-2009), Leipzig, Germany pp. 416-420.21-24 June 2009.
[6] Lin Yang; Jinhua Guo; Ying Wu; "Channel Adaptive One Hop Broadcasting for VANETs," 11thInternational IEEE Conference onIntelligent Transportation Systems, 2008. (ITSC-2008), Beijing, China, pp.369-374, 12-15 Oct. 2008.
[7] Ping Chung Ng; Soung Chang Liew; , "Throughput Analysis of IEEE-802.11 Multi-Hop Ad Hoc Networks," IEEE/ACM Transactions on Networking , Vol.15, No.2, pp.309-322, April 2007.
[8] Information about Connect&Drive Dutch project: http://www.ctit.utwente.nl/research/projects/national/senter/connect-drive.doc/.
[9] Schmidt-Eisenlohr, F.; Torrent-Moreno, M.; Mittag, J.; Hartenstein, H., "Simulation Platform For Inter-Vehicle Communications And Analysis Of Periodic Information Exchange," 4thIFIP/IEEE Conference on Wireless On Demand Network Systems (WONS-2007). Oberguyrgl, Austria, pp.50-58, 24-26 Jan. 2007.