# A Framework for Efficient Communication in Hybrid Sensor and Vehicular Networks

Soufiene Djahel and Yacine Ghamri-Doudane
ENSIIE, 1 Square de la Résistance, 91025 Evry Cedex, France
{soufiene.djahel, yacine.ghamri}@ensiie.fr

*Abstract*—Fast transmission of event-driven warning messages and energy conservation are primary concerns to design robust Hybrid Sensors and Vehicular Networks (HSVNs). In last few years, several protocols have been proposed to address these issues. However, the tradeoff between energy consumption and latency has not been carefully studied and sometimes it is given higher priority than event detection efficiency which remains the first objective of HSVNs. Unlike the existing works, we propose a framework that provides equilibrium between the following three metrics of HSVNs; dangerous events detection, energy consumption and transmission delay. The main advantage of our framework is its ability to ensure an effective detection of dangers on the road and timely transmission of the corresponding warning messages towards the passing by vehicles. This is achieved through the proposed mechanism to switch the sensors' status between sleep and active modes as well as the devised communication scheme between WSN-Gateway and the vehicles cluster head. The preliminary simulation results confirm the effectiveness of our framework and encourage us to pursue further investigation to extend it.

*Keywords* – VANETs, WSNs, HSVNs, Communication protocols .

## I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) [11] are new paradigm of wireless communications that aim to exploit the recent advances in wireless devices technology to enable intelligent inter-vehicle communication. VANETs are distinguished from other wireless networks by their specific characteristics such as; predictable vehicles movement and high speed, powerful processing units, large storage capacities and new applications scenarios. VANETs may also ensure wide dissemination of data and safety related information due to the large transmission range of vehicles and the specific routing protocols used like GPSR [1], BROADCOMM [2] and GEOCAST routing approach [3]. Moreover, as compared to other wireless networks VANETs are not affected by strict energy constraints since the vehicle's battery can provide a long duration energy supply. Although, VANETs are unable to ensure connectivity between vehicles in certain circumstances like in rural areas where the network density is low. VANETs may also not guarantee timely detection of dangerous road conditions due to the high mobility of vehicles.

In contrast to VANETs, nodes in Wireless Sensor Networks (WSNs) [4] are usually static, equipped with scarce energetic resources as well as low processing and storage capacities. Despite that, these sensor nodes are known by their high efficiency in detecting events. They ensure precise and persistent events detection and due to their small size they can be deployed inside road environments to monitor and report the road conditions.

According to the above discussion, we remark that VANETs and WSNs have complementary characteristics, so each of them can benefit from the strengths of the other network while compensating its weaknesses. As a consequence, a new concept of Hybrid Sensor and Vehicular Networks (HSVNs), that merges VANETs and WSNs, has been recently introduced and attracted a lot of attention from both industry and academia. The main goal of HSVN is to enhance the transportation safety through reducing the number and severity of accidents. Furthermore, it may also help the insurance companies as well as the police men investigation by providing useful information regarding the road conditions and vehicle speed at time of accident. We foresee that HSVNs will play a fundamental role in developing Intelligent Transportation Systems (ITS) applications and will be the corner stone for new set of applications that will appear as a consequence of this concept.

In HSVNs, the sensors are deployed along the road to monitor and gather information regarding the weather conditions (ice fall, rain), traffic congestion on a road segment, hidden obstacles, etc. Later on, the passing vehicles are warned about the detected danger if any, through the warning messages sent by the WSN sink (Gateway). The receiver vehicle (usually the leader of a group of vehicles organized in cluster) spreads these messages to the other vehicles using the well known dissemination protocols for inter-vehicles communication. As soon as the driver is aware of the danger, he will adapt his driving skills and speed to prevent or at least alleviate the accident fatalities. In order to contribute to the improvement of the efficiency of HSVNs, we mainly focus, in this paper, on the design of a framework that provides reliable and timely dissemination of the detected dangers from the roadside sensors towards the passing by vehicles. To this end, our framework must fulfill the following requirements:

- Ensure low delay and reliable transmission from WSN towards VANETs.
- Design of energy efficient protocol for inter-sensors communication.
- Propose flexible, scalable and cost effective architecture.
- The proposed architecture of HSVNs should be viable in real scenario.

Due to pages limitation, we will give a global overview of our proposed framework along with a brief description of the functioning of each of its components. However, more details about each component will be presented in our future works.

The remainder of the paper is organized as follows. Section II gives an overview of the existing HSVNs' communication protocols. Next, we provide a detailed description of our framework in section III. In section IV, we present and discuss the preliminary simulation results. Finally, we conclude in Section V.

## II. RELATED WORK

In last few years, some works have been conducted to design reliable and energy efficient communication protocols for HSVNs. However these works have some drawbacks, which we will highlight hereafter, that prevent them from ensuring efficient detection of dangerous events and timely transmission of corresponding warning messages to the vehicles (drivers).

Weingrtner et al [10] have described a prototype for HSVNs and addressed the different types of communication that may exist. Their work provides a global overview on HSVNs and addresses the main challenges that may arise as a consequence of this new architecture.

In order to investigate the feasibility of such network architecture, a field test has been conducted and shown very promising results. This work can be considered as a first step towards a deeper study and analysis to design solutions that guarantee reliable, low delay and energy efficient transmission from the event detector sensor to the WSN-Gateway, as well as fast dissemination of the warning messages within VANETs. Notice that the authors didn't provide any solutions to realize the aforementioned objectives of HSVNs.

A more detailed work has been done in [8] by C.T. Barbara et all. The authors have proposed a communication protocol between the WSN-Gateway and the passing by vehicles. In this protocol, a two way connection should be established between the WSN-Gateway and the vehicles' cluster head before starting data transmission. This may decrease the time devoted for data transmission especially in case of high collision rate or if the WSN-Gateway sends some images regarding other intersections or road segments that the vehicle should cross to reach its destination. Furthermore, the data or images are exclusively sent to the cluster head vehicles, which may jeopardize the safety of drivers and passengers of other vehicles if an event is detected after the cluster head has left the WSN-Gateway transmission range.

Another architecture for HSVNs has been conceived in [5] wherein a duty cycle scheduling scheme based on Time Division Multiple Access (TDMA) is used to reduce the transmission delay from a detector sensor to the WSN-Gateway. This scheme suffers from the same weaknesses of the previous one. Additionally, its main drawback is the periodic broadcast of beacons by the WSN-Gateway, which leads to quick depletion of its energy especially when the role of gateway is fixed. To optimize energy consumption, the authors suggest that the sensors stay in sleep mode and wake up upon request from the WSN-Gateway. This request is sent whenever an approaching vehicle is detected. Indeed, this will save the energy however some dangerous events that may occur during the sensors sleep time cannot be detected. These undetected events are useful to warn the drivers that a given area has recently experienced a danger (e.g., rock falls, animal crossing the roads ...), then they increase their vigilance in order to prevent any surprising events or at least alleviate their impact.

## III. THE PROPOSED COMMUNICATION PROTOCOL IN HSVNs

In HSVNs, we distinguish three different types of communication, each of them follows specific rules and aims to accomplish a special task, as stated below.

- Inter sensors communication aims to ensure reliable event detection and fast event report to WSN-Gateway.
- WSN-Gateway to vehicle communication is responsible for timely report of any detected event to the approaching vehicles which in their turn send back the received warning messages to other WSN-Gateways on the road to their destinations. So, this will allow redundant storage of warning messages and increase the prevention level. For example, the stored messages are used to warn the vehicles traveling in the opposite direction before they approach the dangerous area.
- Inter vehicles communication ensures the dissemination of the warning messages gathered from WSN-Gateways to the whole VANET.

In our framework, the above communication types are not considered as autonomous components independents from each other, but they are designed to interact and complement each other. This way, the workload assigned to WSN is alleviated significantly, at the expense of VANET, and its lifetime is extended.

In what follows, we give a detailed description of the functioning of these communication types.

### A. Sensors to sensors communication

We propose that all the sensor nodes are active during WSN initialization period, then a subset of them remains active and the rest go to sleep until they are requested to wake up again by the WSN-Gateway. This subset should cover the critical region that has recently experienced some events like ice fall, animals crossing the road, falling stones or rocks in mountainous areas, or simply in dangerous turn. A simple way for the WSN-Gateway to choose this subset is to keep a list $L$ of the last $N$ sensors that have reported dangerous events. Afterwards, if the frequency of reporting events from a sensor $s$ is deemed to be high then the WSN-Gateway adds the two direct neighbors of $s$ to this list in order to ensure timely detection of any event that may occur within the region around $s$. The purpose of increasing the number of awake sensors in this region is to prevent any surprising event that may suddenly occur when a vehicle pass by this road segment, particularly in rural areas, and threaten the driver and passengers safety. To summarize, we aim, through this design, to increase the safety level by predicting the possible danger that may arise through recording the historic of events occurred in a given road segment. Afterwards, we use this historic for prevention purposes.

In our Framework, a sensor node that has been requested by the WSN-Gateway to go to sleep will periodically (period = $\rho$ $\mu$s) switch between sleep mode and medium sensing. That is, it stays for ($\rho$-1) $\mu$s in sleep mode, and subsequently senses the medium during 1 $\mu$s. If a signal is detected, then it becomes active for the subsequent $\rho$ $\mu$s and remains so till it receives the frame sent to it. Therefore, when the WSN-Gateway wants to wake up a sensor it should send a packet whose the size is at least equal to $\rho$ $\mu$s. Thereby, the wake up request will definitely be received by the intended sensor.

Another noteworthy feature of our framework, as compared to the works presented in section II, consists in sharing the burden of WSN-Gateway role between a predefined set of sensors, each of them is candidate to fulfill this role during the WSN lifetime. Those candidates accomplish the task of WSN-Gateway either periodically or following a predefined algorithm and for a fixed period of time. Due to the unpredictable events occurrence time and location as well as the random nature of vehicles arrival within the WSN-Gateway's transmission range, we have opted for an algorithm that takes into account the energy level of each candidate sensor and try to keep them operational within the WSN for long duration. Notice that when a candidate sensor becomes a WSN-Gateway, it receives the list $L$ along with any new warning message that has been received from the passing vehicles. Thereby, the crucial information contained in these messages along with the list $L$ are redundantly stored and can be easily recovered later. For more details, our sensor to sensor communication principle is summarized by the algorithm 1.

Since the warning message header shown in Figure 1 is exclusively added by the WSN-Gateway then the intermediate sensors relaying the detector sensor with WSN-Gateway forward a smaller packet. As a result, the transmission delay and the energy consumption are decreased.

***Intra WSN transmission:*** To reduce the end to end delay of warning messages transmission from a detector sensor towards the cluster head vehicle, we should first minimize the maximum delay induced from the transmission of this message from the event detector sensor to the WSN-Gateway. To this end, we propose to use directional antennas rather than the omnidirectional ones. This choice is motivated by the results of the study done in [9], where the authors have demonstrated that the use of directional antenna can extend the transmission range by a factor equals to

$(\frac{4}{tan^2\frac{\theta}{2}})^{\frac{2}{\alpha}}$, where $\theta$ is an angle representing the main beamwidth of the directional antenna and $\alpha$ is the path loss factor, as compared to the case of omnidirectional antenna. Hence, this allows us to monitor the events on a given road segment with less number of deployed

**Algorithm 1** Protocol functioning inside WSN

1: **Initialization period :**
2: For each sensor node $s_i$ set status($s_i$) = active;
3: Upon reception of warning message from $s_i$;
4: Counter-event ($s_i$) ++ ;
5: At the end of the initialization period;
6: For each sensor node $s_i$ do the following;
7: **if** (Counter-event ($s_i$) > $\delta$) **then**
8:   The WSN-Gateway adds $s_i$ to the list $L$;
9: **end if**
10: **End of the initialization period**
11: **Periodic update of the list $L$ by the WSN-Gateway :**
12: Collect statistics about the detected events and the detector sensors;
13: **At the end of each period $P$ do as follows**
14: For each sensor $s_i$ do
15: **if** (Counter-event ($s_i$) > $\delta$) **then**
16:   The WSN-Gateway activates $s_{i-1}$ and $s_{i+1}$ if they are not already active;
17:   Add $s_{i-1}$ and $s_{i+1}$ to the list $L$;
18: **end if**
19: **if** (Counter-event ($s_i$) == 0) **then**
20:   The sensor $s_i$ is requested to go to sleep;
21:   Delete $s_i$ from $L$;
22:   The WSN-Gateway activates $s_{i-1}$ or $s_{i+1}$ if it is not already active;
23: **end if**
$\delta$: this crucial value defines a threshold for the number of triggered events per sensor node. This threshold varies according to the road segment area, i.e rural, mountainous or urban.
$L$: denotes the list of sensors that monitor a dangerous area that has experienced high rate of events.

**Algorithm 2** WSN and VANETs interaction

1: **Upon reception of a beacon or warning-msg from a vehicle :**
2: **if** (CH-beacon received) **then**
3:   CH-beacon processing
4:   Set timeout to $time_{av}$
5:   Decrease the timeout at each time slot
6:   Prepare warning-msg, if any
7:   Send warning-msg to CH-vehicle
8: **end if**
9: **if** (warning-msg received from CH-vehicle) **then**
10:   **if** (it contains fresh information) **then**
11:     Store warning-msg
12:   **else**
13:     Discard warning-msg
14:   **end if**
15: **end if**
16: **if** (timeout reaches 0) **then**
17:   Triggers *cluster head left* event
18: **end if**
19: **Upon reception of a warning-msg from a sensor node :**
20: **if** (warning-msg received) **then**
21:   **if** (*cluster-head left*) **then**
22:     Set *msg-type* to 1
23:   **else**
24:     Set *msg-type* to 0
25:   **end if**
26:   Broadcasts the warning-msg towards VANETs
27: **end if**
$CH - beacon$: refers to the beacon msg sent by the cluster head vehicle (CH-vehicle), through the IEEE802.15.4 interface, to announce its arrival.
We set *msg-type* to 1 to indicate that it is an urgent warning message because the CH-vehicle has left the WSN-Gateway transmission range (i.e, *cluster-head left* is true).

sensors, which leads to significant decrease of the transmission delay since this metric is proportional to the number of sensors separating a reporting sensor and the WSN-Gateway.

### B. Vehicle to sensor and sensor to vehicle communication

Many ITS applications are built on two key messages: namely beacon and event-driven warning. Beacon messages are periodically broadcasted by each vehicle to inform its neighbors about its presence and status. In our framework, we use this beacon message, in addition to its previous role, as a notification of arrival from the vehicles' cluster head to the WSN-Gateway. This notification is transmitted via the IEEE802.15.4 interface of the vehicle since it is equipped with two interfaces (i-e, IEEE802.11P for Vehicle to Vehicle (V2V) communication and IEEE802.15.4 to communicate with the WSN-Gateway).

In order to shorten the connection establishment between the WSN-Gateway and the vehicles' cluster head we modify the format of the beacon broadcasted by the cluster head by adding the following fields:

- Its current speed (the field is calculated as multiple of 5, so we need 5 bits to represent a speed of maximum 130km/h).
- Its Id (identifier)
- The coordinates of its destination

Notice that this modification aims at increasing the time devoted for transmitting useful information from the WSN-Gateway towards the cluster head and reciprocally. Therefore, a larger number of data bytes can be exchanged as compared to the schemes proposed in [5] and [8] which require a longer delay for connection establishment.

Upon reception of the cluster head's beacon, the WSN-Gateway starts counting down a timer equal to the "$time\_av$" value calculated in Equation. 1. Based on the cluster head vehicle speed, the WSN-Gateway calculates the available time for information exchange with the cluster head as follows:

$$time_{av} = (2 * R_{tx}/speed_{CH}) - CHD_{time} \qquad (1)$$

Where $R_{tx}$ is the transmission range of the WSN-Gateway, the $speed_{CH}$ refers to the cluster head vehicle's current speed and $CHD_{time}$ represents the cluster head detection time [1].

---

[1]The cluster head detection time denotes the difference between the reception time of the CH-beacon by the WSN-Gateway and the arrival time of the CH-vehicle within its transmission range.
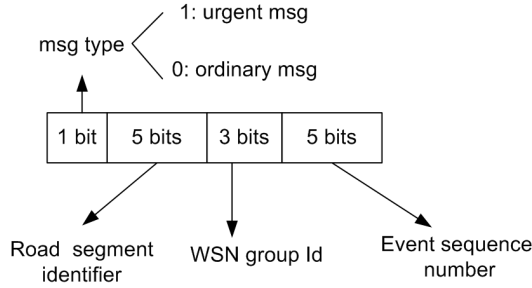
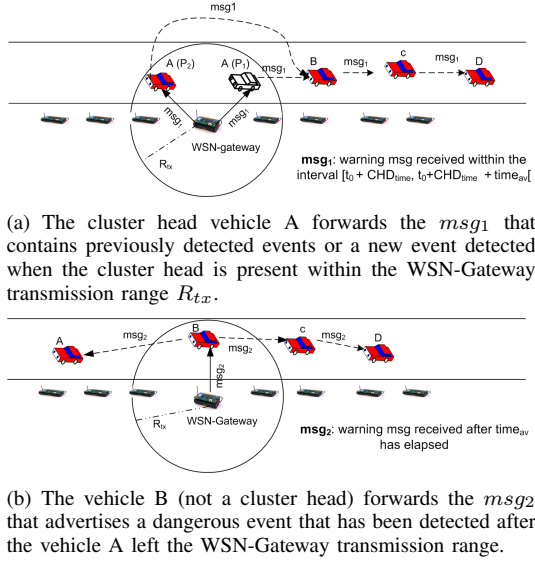Figure 1: Warning message's header added by the WSN-Gateway



(a) The cluster head vehicle A forwards the $msg_1$ that contains previously detected events or a new event detected when the cluster head is present within the WSN-Gateway transmission range $R_{tx}$.



(b) The vehicle B (not a cluster head) forwards the $msg_2$ that advertises a dangerous event that has been detected after the vehicle A left the WSN-Gateway transmission range.

Figure 2: WSN-VANETs interaction

If the warning message advertising the new detected event is received by the WSN-Gateway during the period specified by the interval [2] $[t_0 + CHD_{time}, t_0 + CHD_{time} + time_{av}[$ then it can retransmit it towards the cluster head, as shown in Figure 2(a) where $A(P_1)$ and $A(P_2)$ represent the position at which the cluster head's vehicle is detected and that at which it is going to leave the WSN-Gateway transmission range, respectively. Otherwise, it is transmitted, as an urgent warning message, to any other vehicle (from the same cluster) which is within its transmission range, as depicted in Figure 2(b). The receiver vehicle (for example, vehicle B in Figure 2(b)) will disseminate the received message to all other cluster members including the cluster head. A passing vehicle (not a cluster head) distinguishes an urgent warning message from an ordinary one through the value of the field *msg type* in the message header, as depicted in Figure 1. If this vehicle receives a warning message whose the field *msg type* is equal to 0, it processes and forwards it to the vehicles behind it in the travel direction unless it has already done so (i.e, this message has been already spread through VANET).

To increase the reliability and the energy awareness of our framework, the warning messages received by the vehicles will be re-injected to other WSNs deployed on the nearby or faraway road segments. The objective behind this design is to provide a backup

storage at different points on the road which allows the vehicles coming in the opposite direction to be notified earlier about the danger, if any. Thus, the driver has enough time to reduce the speed and change the direction if necessary. This design has multiple advantages, as stated below:

- Prevent costly transmission of the warning messages between large groups of sensors, so the energy is saved.
- Sensors are deployed only in critical road segments, rather than wide deployments of WSNs which costs much.
- The warning notification is available in multiple WSNs gateways which thus guarantees that all the passing by vehicles are aware of the danger, if any, even if VANETs lose connectivity when the vehicles move out of range, especially in rural areas.

To prevent unnecessary messages processing and storage, when a WSN-Gateway receives a warning message from a vehicle, it first checks if it has been already received or not through comparison of its header with the headers of the stored messages. Moreover, to limit the number of stored messages the WSN-Gateway checks the field "Event sequence number" (see Figure 1) of the received message to ascertain that it contains recent information. If so, then the message is stored and the oldest ones among the stored messages are discarded if the storage capacity has reached its limit. Otherwise, it is discarded.

Algorithm 2 summaries the different steps of the interaction between the WSN-Gateway and the passing by vehicles.

### C. Vehicle to vehicle (V2V) communication

V2V (vehicle to vehicle) communication is an emergent paradigm that necessitates careful analysis and design to fulfill the expected results. In our framework, the role of V2V communication is to ensure large dissemination of the warning messages. To this end, we use a cluster based routing protocol since the vehicles are already organized in clusters for their communication with WSN-Gateways. These clusters are created using the well known clustering algorithms designed for VANETs such as Clustering for Open IVC Networks (COIN) algorithm [6] and LORA_CBF [7].

As for MAC layer, the Wireless Access in Vehicular Environments (WAVE or IEEE 802.11P) protocol is used to allocate spectrum for vehicular communication. However, IEEE 802.11P does not provide sufficient spectrum for reliable exchange of safety related information (like event driven warning messages) among the vehicles. To overcome this weakness of IEEE 802.11P, we are currently exploring the possibilities of applying cognitive radio technology to increase the spectrum allocated to the control channel (CCH) by WAVE, where all safety messages are transmitted. Moreover, as a perspective of this work we plan to propose a robust congestion control mechanism that ensures fast dissemination of the event-driven warning messages received from the WSN-Gateways even in case of high density or traffic jam in the highways.

## IV. SIMULATION RESULTS

Having described the main components of our framework as well as their functioning, we now proceed to measure its performance through a computer simulation using OPNET16.0 [12]. Simulation parameters and configuration of both sensors and vehicles are summarized in the Table I. In order to highlight the effectiveness of our framework, the following metrics have been evaluated.

- Dangerous Events Detection Ratio (DEDR): is the proportion of the detected events to the total number of the occurred ones. This metric is evaluated under the following scenarios.
  - Scenario1: in which our framework is disabled and all the detector sensors are initially in sleep mode, they wake up upon request from the WSN-Gateway as stated in [5]. Vehicles speed and HSVN beacon interval (BI) [3] are varied

---

[2] $t_0$ refers to the arrival time of the vehicles' cluster head within the transmission range of the WSN-Gateway.

[3] the HSVN beacon interval represents the period separating two consecutive transmissions of beacon messages through IEEE 802.15.4 interface to announce the arrival of a vehicle.

to highlight their impact on the DEDR.

- – Scenario2: in this scenario, we assess the impact of the threshold $\delta$, which varies from 1 to10, on the DEDR metric of our framework. This impact is tested under three different periods P (see Algorithm 1) used by the WSN-Gateway to send wake up/sleep requests.

- • We also measure the AWareness Degree (AWD) (under varying vehicles speed and beacon intervals) of the vehicles (drivers) regarding the danger on the road with and without our framework. The AWD is defined as the ratio of the number of warning messages successfully and timely advertised to the drivers to the total number of the detected events by the sensors.

We have simulated a scenario of a motorway with road segments of 10 km length each. This motorway is composed of 4 lanes (2 in each direction). In our simulation, we only focus on one road segment where 5 WSN groups are deployed, each of them covers a road length of 2 km. Events occur randomly in terms of time and location along the road segment. These events will trigger warning messages transmission by the detector sensor. The vehicles are moving along the motorway in both directions while the cluster head ones communicate with the WSN-Gateways of the WSN groups. Average vehicles speed is varied within the range of [25 m/s, 33m/s], thus the available time for exchanging data packets with the WSN-Gateways varies accordingly. The vehicles are equipped with both IEEE802.11 and IEEE802.15.4 MAC protocols since any vehicle can serve as cluster head during its travel and communicate with WSN. To create interferences, we deploy two fixed nodes, near each WSN-Gateway, equipped with IEEE802.11 interfaces and exchange packets of 1000 bytes at the rate of 50 packets/s.

Figure 3 shows the impact of cluster head vehicles speed as well as the beacon interval on the DEDR in baseline HSVN (i.e, HSVN in which our framework is not used). As we can see from the plotted histogram, the DEDR is relatively low since the highest value is equal to 55 % and it is inversely proportional to the cluster head vehicles speed and the beacon interval. We remark also that larger beacon interval (800 ms) leads to an important decrease of the DEDR value. The reason behind this decrease of the DEDR underlies beneath the fact that in case of high speed, the $time_{av}$ decreases significantly and consequently the sensors have less time to detect dangerous events. Moreover, a large beacon interval increases the likelihood that the $CHD_{time}$ gets larger, and thus the WSN-Gateway wake up requests are sent late. Additionally, All the events detected after the cluster head has left the WSN-Gateway transmission range are not transmitted to the rest of the cluster members. This is due to the fact that in the schemes presented in section II the cluster head is the only vehicle that communicates with the WSN-Gateway.

In contrast, as depicted in Figure 4 the DEDR value achieved by our framework is not affected neither by the variation of vehicles speed nor the variation of beacon interval, however the only factor that may affect it is the threshold value ($\delta$) and the Period (P) (see Algorithm 1). The plotted curve reveals that the DEDR value decreases as the threshold value increases till it reaches its lowest value (42 %) when $\delta$ is equal to 10 and the Period is set to 300 seconds. This value represents a decrease of more than the half of DEDR as compared to the case when $\delta = (1, 2, 3)$. This sharp decrease is a consequence of the reduced number of active sensors in a WSN group since the large value of $\delta$ (i.e, 10) and the random nature of event occurrence within the road segment covered by a WSN group leads to lower event detection probability. Moreover, the Period value slightly affects the DEDR which depends mainly on the threshold value. The threshold value is then a crucial parameter since a low value leads to higher DEDR, however it causes also a significant increase of energy consumption of the WSN-Gateway as well as the intermediate sensors due to the large number of wake up requests sent, especially when the WSN size gets larger. On the other hand, a large value of threshold minimizes the energy consumption but

| Parameters | Values |
|---|---|
| Road length | 10km |
| Road lane length | 3m |
| Physical layer | OFDM |
| Transmission range (vehicles) | 250 m |
| Transmission range (sensors) | 80 m |
| No. of sensors in each WSN group | 25 |
| Inter-sensors distance | 60 m |
| No. of vehicles on the road | 10...60 |
| Data rate (for vehicles) | 5.5 mbps |
| Data rate (for sensors) | 250 kbps |
| Simulation time | 1 hour |
| No. of simulation epochs | 5 |

Table I: Configuration of HSVNs parameters

jeopardizes our framework performance as many dangerous events are still not detected. Thus, there is a tradeoff between the desired performance and the energy consumption level, which is hard to manage in order to find an adequate threshold value that satisfies both of these requirements.

To summarize, from these two Figures (3 and 4) we can clearly observe that our framework outperforms the existing schemes (in terms of DEDR value) since, in our framework, this metric is not affected by neither vehicles speed nor beacon interval and can achieve values close to 98 % in the best case, whereas that in the existing schemes achieves only a DEDR of 55 %.

According to the histogram plotted in Figure 5, we observe that, in contrast to DEDR, the AWD is affected by both vehicles speed and beacon interval values. A high vehicles speed reduces significantly the time available for data exchange, especially if lower data rates for IEEE802.15.4 are used (e.g, 20 or 40 kbps). The $time_{av}$ is further reduced when the beacon interval gets higher (e.g. 800 ms or larger). Moreover, the interference caused by the nearby equipments leads to high collision rate and thus the number of warning messages successfully and timely transmitted towards the passing by vehicles is severely affected.

We now compare the AWD of a baseline HSVN with that of HSVN dotted with our framework. To this end, the interference level is reduced and the beacon interval is set to 400 ms to allow more accurate comparison. As we observe from the histogram graphed on the Figure 6, our framework outperforms the baseline HSVN under varying vehicles speeds since the gaps between them in terms of AWD is important. This supremacy of our framework is justified by the fact that in the baseline HSVN all the events detected after the cluster head has left the WSN-Gateway transmission range are not transmitted to the rest of the cluster members. In contrast, in our framework those events are immediately advertised to the next vehicle present within the WSN-Gateway transmission range, thus they are timely delivered to the drivers.

## V. CONCLUSION

A framework for robust communication in Hybrid Sensor and Vehicular Networks (HSVNs) was introduced throughout this paper to overcome the drawbacks of the existing works in the literature. In our framework, we have provided a design guideline for HSVNs aiming to delegate the heavy tasks (in terms of energy consumption and computation) to the vehicles while alleviating the tasks performed by the sensors. Likewise, we have devised a sleep/active mode scheduling scheme, carried out by the WSN-Gateway, which requests a given sensor to wake up or go to sleep according to the assessed danger level of the area around it. So, this ensures high efficiency of events detection and saves the energy as it is consumed only if necessary. The performance of our framework was evaluated using computer simulations and interesting results were obtained in terms of both DEDR and AWD. As future research direction, we would like
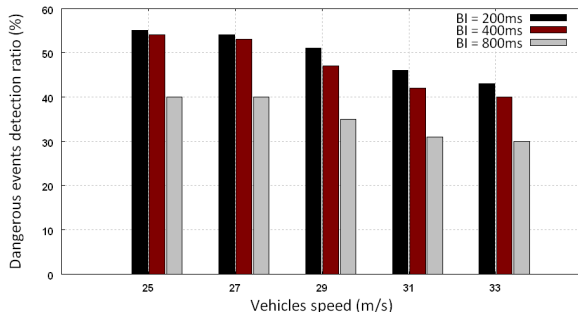
Figure 3: Impact of the cluster head vehicle speed and the HSVN beacon interval (BI) on dangerous events detection efficiency (DEDR): case of baseline HSVN
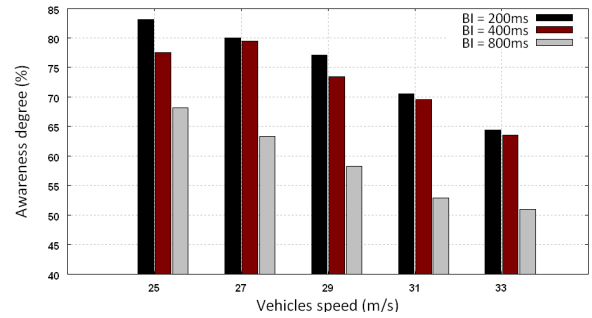


Figure 5: Impact of the HSVN beacon interval (BI) and vehicles speed on the awareness degree (AWD): case of baseline HSVN
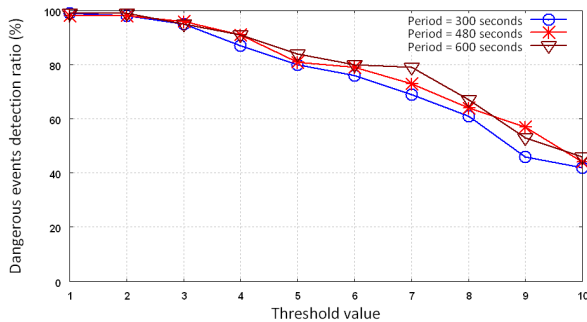


Figure 4: Impact of the threshold value ($\delta$) and the Period (P) on dangerous events detection efficiency (DEDR): case of HSVN using our framework
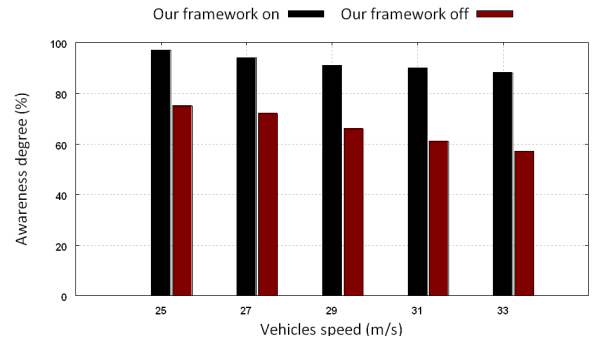


Figure 6: Comparison of the awareness degree (AWD) of a baseline HSVN to that using our framework under low interference with beacon interval equals to 400 ms

to investigate the beacon congestion problem in VANETs in order to prevent delaying the dissemination of the warning messages among the vehicles.

## REFERENCES

[1] B. Karp and H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", *In Proc. of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Boston, Massachusetts, Aug. 6-10, 2000.*

[2] M. Durresi, A. Durresi, and L. Barolli, "Emergency broadcast protocol for intervehicle communications", In Proc. of the $11^{th}$ International Conference on Parallel and Distributed Systems Workshops (ICPADS05), Fukuoka, Japan, Jul. 20-22, 2005.

[3] C. Maihfer, " A survey of geocast routing protocols", *IEEE Communications Surveys & Tutorials, vol. 6, no. 2, pp. 32-42, 2004.*

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, " Wireless sensor networks: a survey", Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[5] H. Qin, Z. L, Y. Wang, X. Lu and W. Zhang, "An integrated Network of Roadside Sensors and Vehicles for Driving Safety: Concept, Design and Experiments", *In Proc. of IEEE International Conference on Pervasive Computing and Communications, (PerCom)*, Mannheim, Germany, Mar. 29 - Apr. 2, 2010.

[6] J. Blum, A. Eskandarian, and L. Hoffman, "Mobility management in IVC networks", *In Proc. of IEEE Intelligent Vehicles Symposium*,Columbus, Ohio, USA, Jun. 9-11, 2003.

[7] R. A. Santos, A. Edwards, R. Edwards, and L. Seed, "Performance evaluation of routing protocols in vehicular adhoc networks", *The International Journal of Ad Hoc and Ubiquitous Computing, vol. 1, no. 1/2, pp. 80-91, 2005.*

[8] C. T. Barba, K. Ornelas and M. A. Igartua, "Performance evaluation of a hybrid sensor and vehicular network to improve road safety", In Proc. of the $7^{th}$ ACM workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN '10), *Bodrum, Turkey, Oct. 17-21, 2010.*

[9] Hong-Ning Dai, "Throughput and Delay in Wireless Sensor Networks using Directional Antennas", In Proc. of the $5^{th}$ International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2009), *Melbourne, Australia, Dec. 7-10, 2009.*

[10] E. Weingrtner and F. Kargl, "A Prototype Study on Hybrid Sensor Vehicular Networks", KuVS Fachgesprch Sensornetzwerke, RWTH-Aachen Technical Report, no. AIB 2007-1, *Aachen, Germany. 2007.*

[11] E. Hossain, G. Chow, V. Leung, R. McLeod, J. Miic, V. Wong and O. Yang, "Vehicular telematics over heterogeneous wireless networks: A survey", Computer Communications, *vol. 33, no. 7, pp. 775-793. Elsevier 2010.*

[12] OPNET Technologies, "OPNET Modeler", http://www.opnet.com/.