International Journal of Information & Network Security (IJINS)
Vol.2, No.5, October 2013, pp. 392~402
ISSN: 2089-3299

A Cooperative Trust Management System for VANET Integrating WSN Technology

Amel LTIFI*, Ahmed ZOUINKHI, Mohamed Salim BOUHLEL***
* Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology of Sfax-Tunisia
** Research Unit: Modeling, Analysis and Control Systems
National Engineering school of Gabes-Tunisia

Article Info

Article history:

Received Jun 12th, 2013
Revised Aug 20th, 2013
Accepted Sep 26th, 2013

Keyword:

VANET
Communication
Trust
Cooperation
WSN
Castalia

ABSTRACT

Vehicle communications are becoming increasingly popular, powered by navigation safety requirements and by the investments of car manufacturers and Public Transport Authorities. The primary VANET's goal is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings or – more generally – telematics information (like current speed, location or ESP activity) which allows to the drivers an early response facing abnormal and potentially dangerous situations like accidents, traffic jams or glaze. In this context, the application of the ambient intelligence technology raises the vehicle capacity to manage its active security. In this article, we propose a new functional model for a vehicle in order to react as an ambient component in its environment. We assume that each vehicle contains a speed sensor. So, a Wireless Sensor Network is created between vehicles. The security state of each vehicle depends on telematics information exchanged periodically between neighbors. We opted to gather the simulations' results of the model with the Castalia-OMNET++ Tools language.

Corresponding Author:

Amel LTIFI,
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology of Sfax-Tunisia
Email: altifi@gmail.com

1. INTRODUCTION

Vehicular Adhoc Network (VANET) has an upcoming potential in the Intelligent Transportation Systems (ITS). VANET can provide many applications to drivers such as security application. This domain attracts the interest of several researches projects and consortiums as the SEcure VEhicular COMmunication project [1] (SEVECOM) which focuses on the security of future vehicles networks, including the security and anonymity of vehicle to vehicle and vehicle to infrastructure communications. The CVIS project [2] aims to develop a communication system that is capable to use a wide range of wireless technologies, the cellular networks (GPRS, UMTS), wireless local area networks (WLAN), microwave short-range communication (DSRC) and infrared (IR) networks. Others project are using the WSN in order to control road security. The problem of road traffic safety is addressed in [3] by integrating the vehicles and road infrastructure with the inexpensive wireless sensor networks (WSNs).

One of the security applications in VANET is the alert management in the case of an accident or an obstacle in the road. In this application, many problems are discussed by researchers as detecting spurious alerts. An algorithm of detecting false alert messages is depected in [4]. This algorithm is based on series of parameters to make a decision about the validity of alert messages. In our case, we implemented a trust management system for alert management.

In order to decrease the probability of occurring accident, each vehicle should alerts other vehicles when it observes an obstacle. Other vehicles may not have a confidence in the vehicle sending the alert. Consequently, it's mandatory to establish a self organizing trust management system [5]. In our case, the role of the certification authority can not be centralized but it is distributed between all vehicles in order to decide about neighbor's trust levels. However, as this information is not relevant for all vehicles, ambient intelligence is considered to be vital for more intelligent inter-vehicular communication.

Most existing Intelligent Transportation Systems (ITS) are using expensive sensors in sensing tasks. Nowadays, there is the technology of Wireless Sensor Networks (WSN) for the same purpose. The application of WSN in ITS, allows a suitable infrastructure for more intelligent and collaborative applications to improve vehicular security.

The main idea of this paper is the proposal of an application of WSNs to such ITS scenarios. For security issues, we propose a model of a trust management system for a self-organised vehicular network. The scenario proposed here is a set of vehicles passing through a road in two ways. Each vehicle equipped at least with a speed sensor. All speed sensors are connected by a WSN. Through this WSN, vehicles transmit their speed values and others useful information. These informations are used by each vehicle to manage its security situation by detecting a dangerous situation or by making a desicion after receiving a warning message based on a trust management model. In order to validate our model, we used the Castalia simulator that is a wireless sensor networks simulator.

The paper is organized as follows: a comparision between WSN and VANET is depicted in the second section. A general idea about vehicles communication is illustrated in the third section. We described by details our cooperatif trust management system in the forth section. The simulation results are announced in the fifth section. And finally, we conclude our paper in the last section.

2. WIRELESS SENSOR NETWORK & VANET

The WSNs consist of a set of devices referred to nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links based on the collaborative effort of nodes. WSNs provide significant advantages both in cost as well as in distributed intelligence [6].

WSN and VANET are both adhoc network. However there are many differences between them. We used a comparison made in [7] between wsn and adhoc networks to build a comparison between WSN and VANET. The table above illustrates this comparison.

Table 1: Wireless Sensor Network VS Vehicular Adhoc Network.

Parameter	**WSN**	**VANET**
Power	Limited	Not limited
Computational capability	Limited	Not limited
Memory	Limited	Not limited
Node deployment	uniformly distributed	Changeable density

VANETs possess some perceptible characteristics that make its nature different from other wireless ad-hoc networks. New challenges are occurred to meet the needs of this type of networks. The design of new especially protocols is among these challenges.

An essential characteristic of VANETs is the high mobility of vehicles that can be up to one hundred fifty kilometers per hour. Furthermore, the topology of a number of VANET changes frequently and unpredictably. For this reason, the time that a communication link exists between two vehicles is very short especially when the vehicles are moving in opposite directions. Another consequence of this high speed quality is that the utility of the exchanged messages is very affected by latency. For example, if we assume that a vehicle is unexpectedly stopping or suddenly stops, it should broadcast a message to warn other vehicles of the probable danger. Considering that the driver needs at least 0.70 to 0.75 sec to initiate his response[1], the warning message should be delivered at virtually zero second latency.

[7] investigates in the application of WSNs to probably ITS scenarios, dealing with the principal problems that may arise when mounting these systems. They concluded that, in the ITS scenario, there are some concerns which have not been addressed yet or incompletely attempted. Security is an example which there are really few specific research works for including it in WSN-based ITS works.

[1] http://www.ukdissertations.com/dissertations/engineering/vanet-technology.php

A new concept of Hybrid Sensor-Vehicular Networks is initiated in [8]. WSN and VANET can profit from the potencies of each other while compensating the weaknesses. Their task can be considered as initial investigation in such systems where yet many challenging issues exist.

Authors in [3] propose methods to establish effective and efficient vehicle-sensor and sensor-sensor interactions. Prototype of the designed system has been implemented and tested. An integrated VANET-WSN system was proposed in this paper to surmount the inherent restrictions of pure VANET-based system. They defined protocols for efficient vehicle-sensor and sensor-sensor interactions.

A framework based on WSN is proposed in [9] aims to resolve the requirements of VANET applications.

3. VEHICLE COMMUNICATION

In self-organized network, the only possible communication is between nodes. In VANET, the vehicle-to-vehicle communication is defined to be the dynamic wireless exchange of data between nearby vehicles capable of short range wireless communication. Enables vehicles to know where the vehicles in its vicinity are and what they are doing. The V2V technology could avoid about of 80% of crashes involving sober drivers, according to The National Highway Traffic Safety Administration (NHTSA)2.

A dedicated short-range communication (DSRC) multi-hop mode is used for V2V communications and exploits the flooding of information of vehicular data applications [10]

This new technology allows vehicles to "communicate" wirelessly to help ensure each driver's safety while on the road. Each vehicle can send information to other regarding its speed, direction, and location. This is meant to avoid accidents by detecting another car before the driver can see it with their own eyes. There are numerous other applications that could benefit from V2V communications. Some are [11]:

- Forward Collision Warning,
- Emergency Electronic Brake Light,
- Blind Spot/Lane Change Warning,
- Intersection Movement Assist
- and Control Loss Warning.

4. COOPERATIVE TRUST MANAGEMENT SYSTEM

4.1. General context

The network architecture is illustrated in figure1.

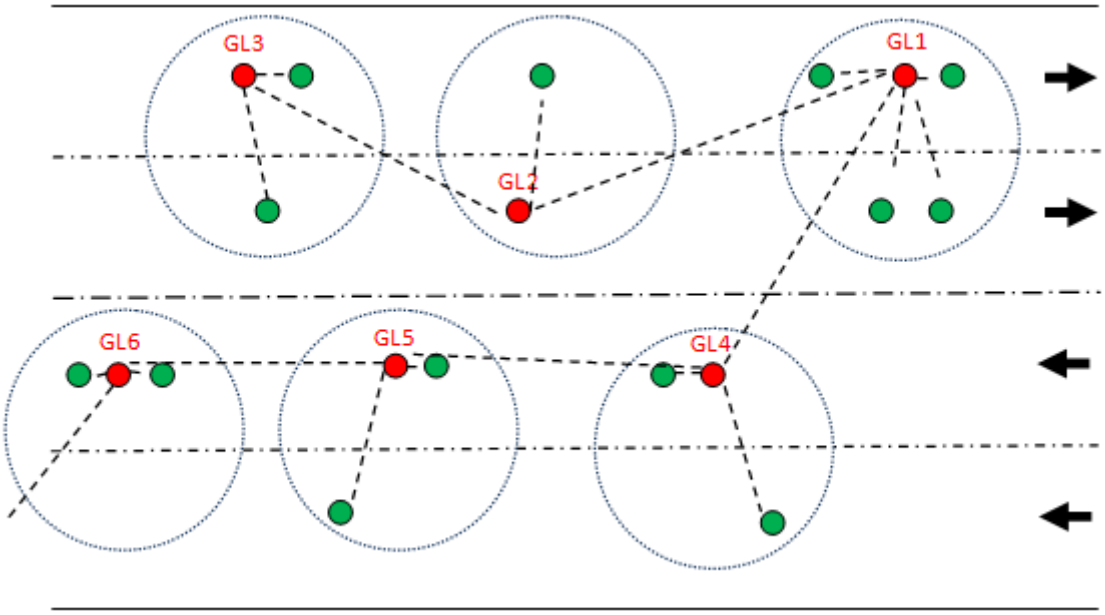

Figure 1: VANET infrastructure.

[2] www.**nhtsa**.gov

Communication between different components of this architecture is achieved through two types of messages: control messages and data messages (in our case the warning messages).

4.2. Functional model

Our model is depicted in figure 2. It handles the trust management in order to construct a healthful community between vehicles on the road. As a result, the road security is increased by exchanging a trusted messages including helpful information about the road status. Vehicles, in our model, are involved to cooperate with their enclosures.

The trust management system is based on a knowledge base to allow to the vehicle to take the appropriate decision on the received warnings about exceptional states in the root. Each vehicle communicates with others vehicles through wireless transmission channel. Therefore, there are two main components that should be integrated in the vehicle: the trust management system and the knowledge base. We described in next sections these two principal components in our architecture.

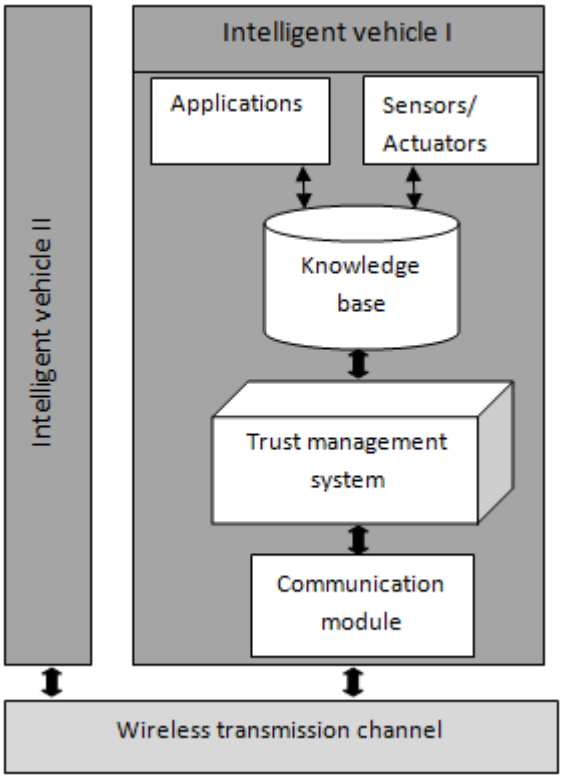

Figure 2: Functional model of the application.

4.3. The knowledge base

A knowledge base is an artificial intelligent tool. We use this tool to attach to the vehicle the ability to make decision. It processes general information of the vehicle (rate, constructor, position, direction, identifier …) and information concerning trust model (reference/local trust model). It depends on the rule of the vehicle i.e. a normal vehicle or a group leader.

VANET is basically a self_organised network. In the absence of a central party, a vehicle should cooperate with its environment in order to make a reasonable decision. For this reason, this network enables information exchange between vehicles [12]. The data collected from the vehicles cooperation is very useful in this case. There are some solutions that use a knowledge base to maintain some important information about environment. SODAD [13] is a technique for scalable information dissemination in highly mobile VANETs. The main applications designed by this technique are weather and traffic information systems. The main idea of this method is that every node maintains a knowledge base, where it stores known information (e. g., road conditions or parking lot occupancies). The nodes periodically send all or parts of their knowledge to their neighbors. Each node, after receiving this knowledge, updates its knowledge base. Step by step a local overview of the total scenario emerges.

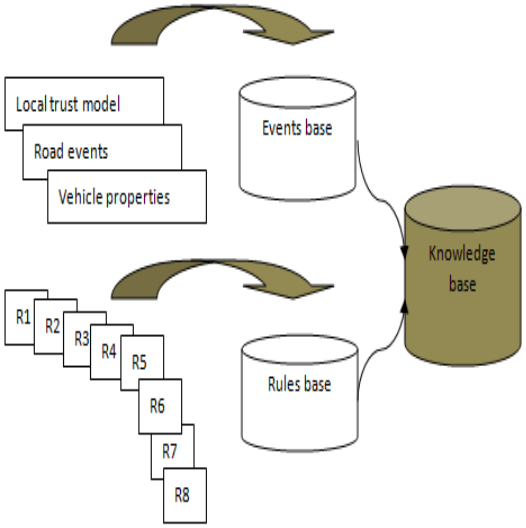

Figure 3: The knowledge base structure.

The aim of this knowledge base is the alert endorsement. Based on the knowledge base, each vehicle can make a decision about the trustworthiness of an arriving alert message. The events base consists of the road events as an accident, the local trust model and vehicle properties as its identifier. The rules base contains eight rules described in [14].

4.4. The trust management system

The trust management system accesses the knowledge base in order to update trust model and to obtain the effective decision about received message correctness. When a vehicle detects a threat from the sensor information or services offered, it sends an ALARM message on broadcast. The receiver vehicle accesses its knowledge base to verify the trust value of the message sender to make the appropriate decision.

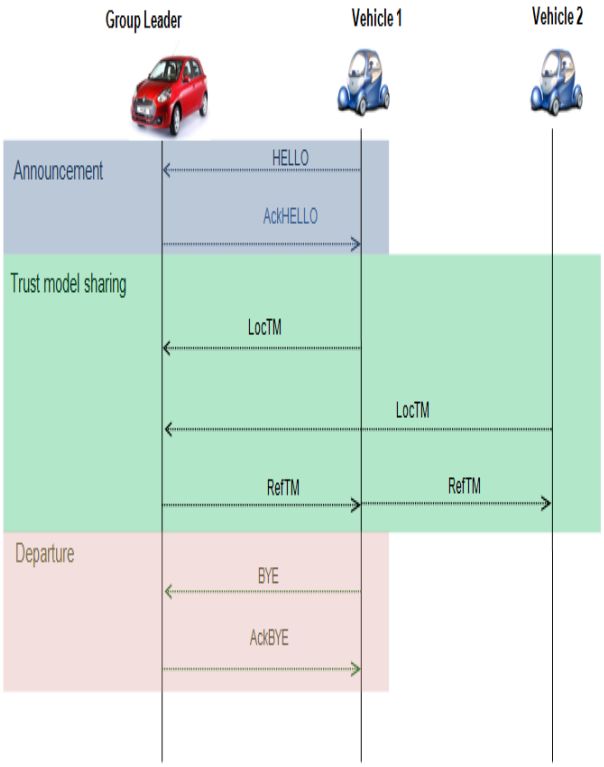

Figure 4: Sequence diagram of messages exchange.

In order to manage and deliver an updated trust model, the trust management system invokes the knowledge database described previously in order to maintain the creation and the exchanging of knowledge used for making decision. A trust model is generated by the trust management system. This trust model is used by vehicles each time it decide on a confidence degree of received warning messages. There are two types of trust models: a reference and a local trust model. Both are integrated in the knowledge base. This trust model contains a trust value for each vehicle in the same group. It's updated by exchanging trust models created by other vehicles. This exchange of trust information is a part of our trust management system. We describe in the following exchanged messages used in our model for cooperation between vehicles community.

The main goal of VANET is to exchange safety information like warning messages. VANET applications applied the rule of periodic exchange of messages between nodes [15]. Vehicles cooperate in order to create a trusted community between them. This cooperation is applied by exchanging messages. We propose a set of messages those used in our trust management system. Main messages are illustrated by a sequence diagram in the figure 3. These messages are classified as follow:

- **Control messages**
  - **HELLO**: it's the first message transmitted by a coming vehicle to a group. The vehicle announces its arrival by sending its identifier.

HELLO	Address(idV)

Figure 5: Strusture of the Hello message.

  - **ACKHELLO**: only the leader answers a new vehicle after receiving its HELLO message. This message contains the identifier of the leader to be used in next communication steps.

ACKHELLO	Address(idLeader)

Figure 6: Structure of the AckHello message.

  - **BYE**: it's transmitted by the vehicle when it decides to leave the group; i.e. the vehicle will be out of the group area.

BYE	Address(idV)

Figure 7: Structure of the BYE message.

  - **GRE**: this is a greeting message, it is sent periodically. It allows calculating distances between vehicles based on the Received Signal Strenth Indicator (RSSI). It contains the location of the sender vehicle (Vx, y), its rate (Vr) and its direction (D).

GRE	Myid	Vx	Vy	Vr	D

Figure 8: Structure of the GRE message.

  - **ALARM**: this message is sent each time when an unexpected event occurs on the road. It contains important information about occurred event as location (Vx, Vy), rate (Vr), time (T) and others information that depend on its type.

ALARM	Myid	idOtherV	Vx	Vy	Vr	T	Others

Figure 9: Structure of the ALARM message.

  - **AckLocTM**: this is the acknowledgment of the LocTM message described below.

AckLocTM	Address(idV)

Figure 10: Structure of the AckLocTM.

  - **AckRefTM**: this is the acknowledgment of the RefTM message described later.

AckRefTM	Address(idV)

Figure 11: Structure of the AckRefTM.

- **Data messages**
  - **LocTM**: this message contains a table representing the local trust model created by the sender vehicle.

LocTM	Data

Figure 12: Structure of the LocTM message.

  - **RefTM**: this message can be sent only by the group leader to other vehicles in the group and to the nearest RSU. It contains a table representing the reference trust model created by the group leader.

RefTM	Data

Figure 13: Structure of the RefTM message.

The local and the reference trust model are calculated by vehicles.

5. Simulation

In our application, we will validate an alert detection application by simulating a network of mobile sensors in the Castalia simulator that is dedicated to wireless sensor networks. The application made through the network detects a danger of accidental state and transmits an alarm message to other nodes. This system can be applied in the field of active safety systems in VANET. The scenario used is a set of vehicles traveling through a highway. Simulated field is a highway with an area equal to 15000mx15m which contains six active vehicles (V0; ... V1, V5), we fixed the vehicle number 4 as the group leader. The following table shows how the arrangement of these vehicles and the speed of each vehicle:

Table 2: Initial road configuration.

Vehicle	V0	V1	V2	V3	V4	V5
Direction	1	1	1	2	1	1
position (x, y) (m)	(1,20)	(6,1)	(1,41)	(11,11)	(6,21)	(1,61)
rate (km/h)	60	60	60	60	60	60

From these parameters that we have indicated in the table 2 above, we represent the following diagram:

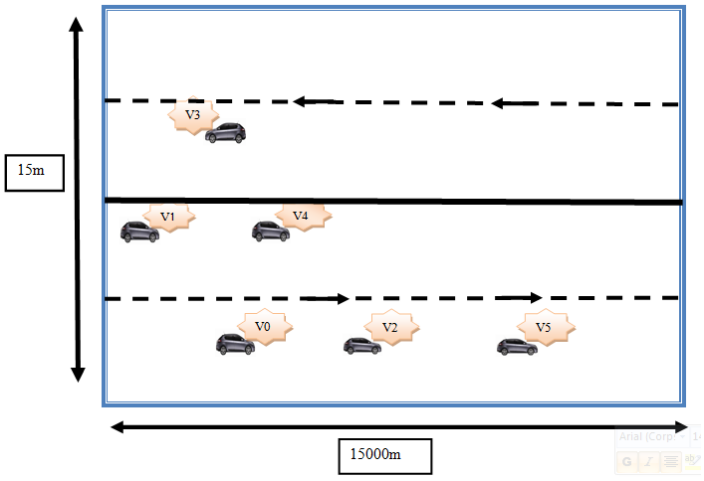

Figure 14: Initial vehicles position.

Among the different types of sensors we choose the speed sensor to detect the speed of each vehicle, for example if there is a vehicle in a shutdown state, the vehicle closest course will explore the problem in the first place and it will give a sign to inform others.

Moreover, in such scenario the vehicles do not circulate freely throughout the region.

- They are in communication with other vehicles.
- They follow the highway segments.

- A mobility model describes the movement pattern followed by the nodes of a specific scenario.
- The choice of appropriate simulation parameters and the model of mobility is crucial for accurate results

Before starting the simulation, as mentioned in table 3, several parameters must be set according to several factors such as the infrastructure parameters configuration (surface, number of nodes, ...), the simulated protocol (packets sent, packet length, ...), the type of sensor selected.

Table 3: Values of configuration parameters.

Names of parameters	Values of parameters
The average speed of nodes	60 km/h
Number of road	4 lanes (two in each direction)
Length of the highway	15000m
Number of mobile nodes	6 nodes
Packet Size	1000 to 2000 bytes
Simulation time	200s
Initial energy	18720
MAC	IEE 802.15 .4

As we mentioned previously, the proposed trust management system is based on cooperation and communication between vehicles in order to manage effectively a dangerous state and to avoid a possible accident by transmitting right information. The figure 15 shows the number of received packets between nodes during the simulation time.

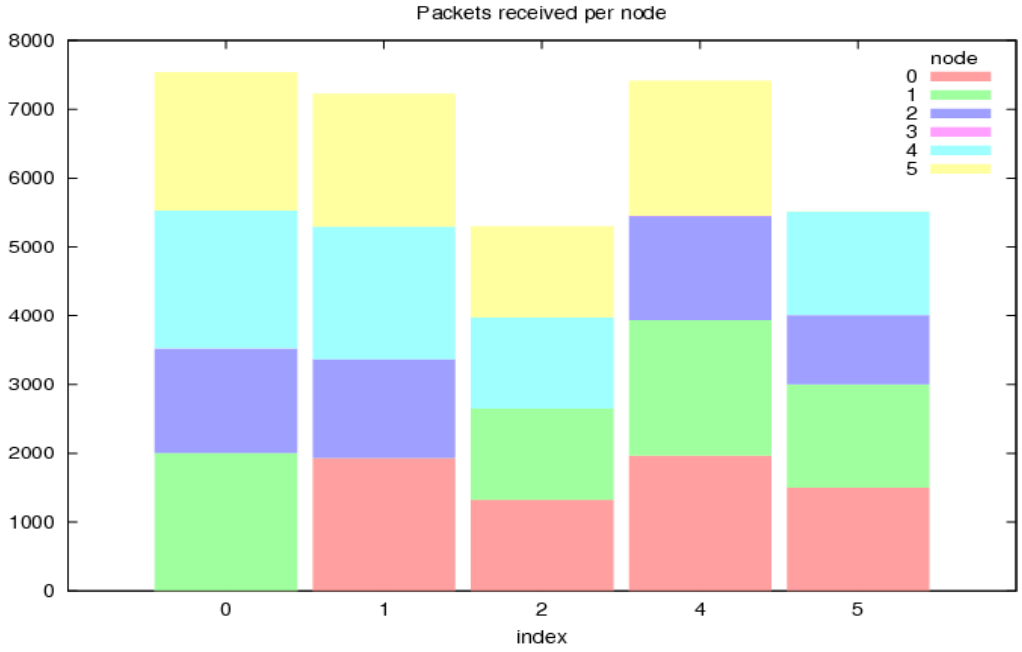

Figure 15: Received packets per node.

The figure 15 shows that the node number 3 did not send packets to others vehicles. But in the reality, it sent only a negligible number of packets because its trajectory is limited.

In order to evaluate our model, we are implemented some specific scenario in each one we modify some configuration parameters. We described below these scenarios and their simulation results.

5.1. Scenario1:

Each node should announce its presence in the group area. First, it should send the HELLO packet on broadcast. After, it waits to be acquitted from the group leader. In our case, the vehicle number 4 is the group leader. When it is aquitted, it enters in communication with group members by sending the GRE packet. In figure 16, the vehicle number 0 send the HELLO packet and it's aquitted at t=0.030139895216s, it begins to send the GRE packet at t=0.231451892386s.

```
at t = 0.028839895217  SN.node[4].Application   4 has received from 0 :   packet = HELLO
…
at t = 0.030139895216  SN.node[0].Application   0 has received from 4 :   packet = ACKHELLO
…
at t = 0.231451892386  SN.node[3].Application   3 has received from 0 :   packet = GRE
…
at t = 0.231451892386  SN.node[1].Application   1 has received from 0 :   packet = GRE
…
at t = 0.231451892386  SN.node[2].Application   2 has received from 0 :   packet = GRE
…
at t = 0.231451892386  SN.node[4].Application   4 has received from 0 :   packet = GRE
…
at t = 0.231451892386  SN.node[5].Application   5 has received from 0 :   packet = GRE
```

Figure 16: Exchanged packets in the scenario of the entering of node 0 to the group.

5.2. Scenario 2:

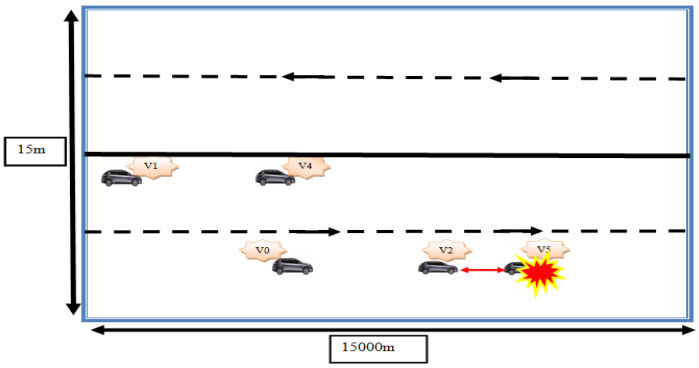

Figure 17: The scenario of the occuring of an obstacle in the road.

In this scenario, the vehicle number 5 will be stopped at t=150s. So, it will be an obstacle to the vehicle number 2 as shown in figure 17 at t=150.014873386684s, the vehicle number 2 receives from vehicle 5 a GRE packet.

```
at t = 150.014873386684SN.node[2].Application   2 has received from 5:          packet = GRE
…
at t = 150.014873386684SN.node[2].Application   alert state detected by node2 obstacle after 6m
…
at t = 150.016173386683SN.node[4].Application   4 has received from 2:          packet = ALARM
…
at t = 150.016173386683SN.node[4].Application   Trusted alarm message received from 2
…
at t = 150.017473386682SN.node[0].Application   0 has received from 4:          packet = ALARM
…
at t = 150.017473386682SN.node[0].Application   Trusted alarm message received from 4
…
at t = 150.017473386682SN.node[1].Application   1 has received from 4:          packet = ALARM
…
at t = 150.017473386682SN.node[1].Application   Trusted alarm message received from 4
…
at t = 150.116176657988SN.node[0].Application   0 has received from 2:          packet = ALARM
…
at t = 150.116176657988SN.node[0].Application   Trusted alarm message received from 2
…
at t = 150.116176657988SN.node[1].Application   1 has received from 2:          packet = ALARM
…
at t = 150.116176657988SN.node[1].Application   Trusted alarm message received from 2
```

Figure 18: Exchanged messages in the scenario 2.

The vehicle 2 calculates the distance between it and the stopped vehicle 5. It finds that the distance is 6m that is inferior to the minimal distance defined in the implementation (Dmin = 10m). In this case, it sends an ALARM message on broadcast as mentioned in figure 18. The vehicle 2, in this case, is a trusted vehicle.The figure 18 shows that node 2 has detected this problem since it is the closest to node 5 so it sends an "ALARM" message on broadcast. So in this case each node receiving the alarm message from node 2 will retransmit it to its neighbors.

5.3. Scenario 3

In this scenario, vehicles are in the same situation as in the scenario 2. The only difference is that the vehicle 2 is now an untrusted vehicle.

```
…
at t = 150.014873386684SN.node[2].Application    2 has received from 5:    packet = GRE
…
at t = 150.014873386684SN.node[2].Application    alert state detected by node2 obstacle after 6m
…
at t = 150.016173386683SN.node[4].Application    4 has received from 2:    packet = ALARM
…
at t = 150.016173386683SN.node[4].Application    Untrusted alarm message received from 2
…
at t = 150.116176657988SN.node[0].Application    0 has received from 2:    packet = ALARM
…
at t = 150.116176657988SN.node[0].Application    Untrusted alarm message received from 2
…
at t = 150.116176657988SN.node[1].Application    1 has received from 2:    packet = ALARM
…
at t = 150.116176657988SN.node[1].Application    Untrusted alarm message received from 2
…
```

Figure 19: Exchanged messages in the scenario 3.

As shown in figure 19, the node 4 didn't retransmit the ALARM message to other vehicles. The reason is that the vehicle 2 is not trusted.

6. Conclusion

In this paper, we described a new application of road security that integrates two types of adhoc networks: the Wireless Sensor Network and the Vehicular Adhoc NETwork. The main aim of this application is the detection of the road obstacles and to communicate this information in a trusted and a self-organised environment. We integrated the WSN technology because it allows a suitable infrastructure for more intelligent and collaborative application. First, we defined our trust management model which is based on specified rules defining the exchanged messages between vehicles' groups. Second, for validation purposes, we implemented our model under the Castalia simulator. We concluded finally that our model functionalities are attended and vehicles behaved as described in our model. Our new model can be useful to manage an alert state in the road in case of a self-organized vehicular network where there is any trusted third party.

REFERENCES

[1] P. Papadimitratos et al., "Secure Vehicular Communications: Design and Architecture", *IEEE Communications Magazine*, vol. 46, pp. 100-109, Nov 2008.

[2] D. Gruyer et al., "Robust positioning in safety applications for the CVIS project", *Intelligent Vehicles Symposium*, pp. 262-268, 2010.

[3] H. Qin et al., "An integrated network of roadside sensors and vehicles for driving safety: Concept, design and experiments", *in IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Mannheim, Germany, March 29 - April 2, pp. 79 –87, 2010.

[4] M. Aamir and S. Mukhi, "Algorithm to Detect Spuriou Communications in Vehicular Ad hoc Networks", *International Journal of Information & Network Security (IJINS)*, June, Vol.2, No.3,pp. 239~244, 2013.

[5] P. Wex et al., "Trust Issues for Vehicular Ad Hoc Networks", *67th IEEE Vehicular Technology Conference (VTC2008-Spring)*, Marina Bay, Singapore, May 11–14, pp. 2800-2804, 2008.

[6] F. Losilla et al., "A Comprehensive Approach to WSN-based ITS Applications: A Survey", *Sensors conference 2011*, October 28, 2011.

[7] Radhika.K et al., "Applications of WSN in VANET", *National Conference on Recent Trends in Engineering & Technology*, B.V.M. Engineering College, V.V.Nagar,Gujarat,India, 13-14 May, 2011.

[8] E. Weingärtner and F. Kargl, "*A Prototype Study on Hybrid Sensor-Vehicular Networks Ext. Abstract"*, AIB 2007-11, RWTH-Aachen, Aachen, Germany, July 2007.
[9] R. A. Khan et al., "Wireless Sensor Networks: A Solution for Smart Transportation", *Journal of Emerging Trends in Computing and Information Science*, vol.3, April 2012.
[10] A.M. Vegni and T.D.C. Little, "Hybrid Vehicular Communications based on V2V-V2I Protocol Switching", *Intl. Journal of Vehicle Information and Communication Systems (IJVICS*), Vol. 2, Nos. 3/4, pp.213–231, 2011.
[11] B. Xu et al., "Monitoring neighboring vehicles for safety via V2V communication", *2011 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, Beijing, China, July 10-12, 2011.
[12] M. Jerbi, et al., "Vehicular Communications Networks: Current Trends and Challenges", *In Handbook of Research on Next Generation Mobile Networks and Ubiquitous Computing*, IGI-Global, 2010.
[13] L. Wischhof et al., "Information Dissemination in Selforganizing Intervehicle Networks", *IEEE Transactions on Intelligent Transportation System*, vol 6, pp. 90–101, March 2005.
[14] A. LTIFI et al., "An alert endorsement through cooperative trust management for VANET", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 10, No. 4, April 2012.
[15] J. Grover et al., "Machine Learning Approach for Multiple Misbehavior Detection in VANET", *First International Conference on Advances in Computing and Communications (ACC-2011)*, July. 22-24, Kochi Kerala, India, pp. 644-653, 2011.

BIOGRAPHIES OF AUTHORS

Amel Ltifi is a PhD student at the National Engineering School of Sfax (Tunisia) and a member of Sciences and Technologies of Image and Telecommunications (SETIT) laboratory. She received the National engineering Degree from the National School of Informatic sciences (ENSI), Tunisia in 2003 in computer sciences. She received the Master degree from the Higher School of Informatics and Multimedia of Gabes (ISIMG), Tunisia, in 2010. Her research activities are focused on Distributed Systems, Ambient Intelligence systems and architectures, VANET and Wireless Sensors Network Concepts.

Ahmed Zouinkhi is Associate Professor at the National Engineering School of Gabes (Tunisia) and a member of Modeling, Analysis and Control Systems (MACS) laboratory. He received the Notional engineering Degree from the National Engineering School of Monastir (ENIM), Tunisia in 1997 in industrial computing. He received the DEA degrees and the CESS (certificate high specialized electrical study) from the Higher School of Sciences and Techniques of Tunis (ESSTT), Tunisia, in 2001 and 2003, respectively. He received his PhD degree in 2011 in Automatic Control from the National Engineering School of Gabes (Tunisia) and a PhD degree in Computer Engineering from the Nancy University (France). His research activities are focused on Distributed Systems, Smart Objects theory and applications, Ambient Intelligence systems and architectures, RFID, VANET and Wireless Sensors Network Concepts and Applications in manufacturing and supply chain.

Mohamed-Salim BOUHLEL was born in Sfax (Tunisia) in December 1955. He received the engineering Diploma from the National Engineering School of Sfax (ENIS) in 1981, the DEA in Automatic and Informatic from the National Institute of Applied Sciences of Lyon in 1981, the degree of Doctor Engineer from the National Institute of Applied Sciences of Lyon in 1983. He has received in 1999 the golden medal with the special mention of jury in the first International Meeting of Invention, Innovation and Technology (Dubai). He was the Vice President of the Tunisian Association of the Specialists in Electronics. He is actually the Vice President of the Tunisian Association of the Experts in Imagery and President of the Tunisian Association of the Experts in Information technology and Telecommunication. He is the Editor in Chief of the International Journal of Electronic, Technology of Information and Telecommunication, Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication: (SETIT 2003, SETIT 2004 ,SETIT 2005, SETIT 2007, SETIT 2009 and SETIT 2012) and member of the program committee of a lot of international conferences. In addition, he is an associate professor at the Department of Image and Information Technology in the Higher National School of Telecommunication ENST-Bretagne (France).