Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

A. Peinado, A. Ortiz-García, J. Munilla
Dept. Ingeniería de Comunicaciones
E.T.S. Ingeniería de Telecomunicación, Universidad de Málaga
Málaga, Spain
apeinado@ic.uma.es, aortiz@ic.uma.es, munilla@ic.uma.es

***Abstract*—In this work, we present a distributed system designed for road traffic management. The system is inspired by the behavior of the ant colonies. The distributed design responds to the particular limitations of an emergency situation; mainly, the fixed infrastructures are out of service because no energy supply is available. The implementation is based on the VANET facilities complemented with passive RFID tags or GPS localization. The vehicles can use the information of previous vehicles to dynamically decide the best path. A scale prototype has been developed to validate the system. It consists of several small size robotic vehicles, a test road circuit and a visual monitorization system. The security of the system is provided by a combination of data aggregation and reputation lists.**

Keywords - security;emergency;reputation lists;ant colonies; road traffic;RFID;VANET;robotic vehicles

I. Introduction

Currently, road traffic management systems are based on centralized strategies that use a variety of technologies, such as cameras and sensors to obtain information about the actual traffic state. The data are analyzed in a data processing center where decisions are made and communicated to the operational services and the drivers through panels and displays located on the road itself. An example is the panels that inform drivers of the maximum speed on motorways and highways to access certain cities, which varies depending on traffic conditions [3], [15].

In emergency situations, it is very common that telecommunications networks do not work properly, mainly affected by falling energy sources that feed the fixed infrastructure of these networks. Consequently, although the data processing centers have alternative power sources, and even their own networks for data communication, the lack of energy affects the cameras and sensors in a very high percentage.

In this paper, we propose a system for road traffic management which can continue to operate when the energy supply is not available for the infrastructure, in short, a system that does not rely on such infrastructure to reach the objective. This system is mainly supported on the advantages of vehicular networks (VANETs), as no external energy supply is needed.

Vehicular ad hoc networks (VANETs) [6] are presented as a generation of networks oriented to improve the safety and driving comfort. These networks allow connectivity among mobile hosts (vehicles). This way, vehicles in a VANET can share information to each other in a short range by using WAVE wireless protocol, *i.e.*, the IEEE 802.11p technology [7]. This communication between nodes is named V2V (for vehicle-to-vehicle).

The use of a light infrastructure or a backup network is also considered in VANET scenarios as a mean to improve the services offered by the network providing the so called vehicle-to-infrastructure communication (V2I or I2V).

The vast majority of defined and developed applications in VANETs are related to road safety, and are based on the transmission of information between vehicles on accidents, congestion levels in certain parts of the road, signaling dangerous sections, etc.. Sometimes the information is generated in a vehicle that begins to transmit it to the others. Other times the information is generated in the infrastructure and transmitted through the Road side units (RSU) [1].

These architectures also allow the development, in a natural way, of traffic management systems getting information about the current traffic and informing drivers instantly. However, the use of the infrastructure represents a risk to consider in emergency situations [15].

Accordingly, the traffic management system should be based only on V2V communications. We proposed such a system, in which every vehicle decides the path at each node (crossroad) using the information provided by previous vehicles following a procedure inspired by the behavior of the ant colonies.

Section II describes the proposed model for road traffic management inspired by the ant colonies. Section III focuses on the security aspects of the proposed system. Sections IV and V deal with the implementation details and a scale prototype performed to validate the system and demonstrate its operation. Section VI describes the results and future work.

II. Model inspired by Ant Colonies

Taking into account the particular conditions of emergency situations, it seems reasonable to implement a management algorithm that can be performed in a distributed

ISBN: 978-1-61208-298-1

manner, *i.e.*, through the collaboration of the vehicles themselves, without the need for fixed infrastructure.

Therefore, in this paper, we propose the use of a system based on the behavior of ant colonies [5]. While there are numerous algorithms for transport and logistics based on this principle, all of them are applied in simulation and optimization tasks, in order to calculate the *a priori* best routes [4],[17]. The present proposal is a direct implementation of the algorithm used by ants to search for food. This implementation allows the vehicles to choose the suitable route in real-time while drive on the road.

In general terms, each ant initially chooses a random walk from the nest in search of food. When an ant finds food, it leaves a trail of pheromones on their way back to the nest so that the other ants can follow it. This substance disappears as time passes. This fact allows the ants always decide to follow the path with the higher level of pheromone. Thus, all ants end up finding the shortest path to the food.

This operating principle can be applied, with some minor modifications, to control the road traffic, providing every vehicle with the capacity to leave a "trace" and detect the presence of "pheromone"; that is, providing a distributed mechanism without the help of a fixed infrastructure. The goal, in this case, would not be to find the shortest path, but properly distribute the traffic so as to reduce overall congestion level, and sometimes, as in emergency cases, help the vehicles to find the available routes.

The main modifications to be applied to the original algorithm are the followings.

A. Route selection

Provided that the vehicles have the ability to detect a trail of pheromones, unlike ants, vehicles should choose the path with lower level of pheromones. In this way, the vehicles could be distributed uniformly avoiding large concentrations along the same route.

It is important to note that the choice of the route is done by the driver finally. This means that the algorithm only informs the driver about the route he should take. If the driver chooses not to follow the recommendation, the system also operates properly as the pheromone trail detected by other vehicles will always corresponds to actual state of the road, as the vehicles leave the trail on the route they are really driving.

Moreover, the criterion for choosing the recommended route may be configurable in order to meet the different needs of users. Sometimes the vehicles may be interested to take the road less congested and other times, in emergency situations, it may be more efficient that everyone follows the same route, because it is probably the only one available.

B. Trail generation

The trail of pheromone should be emitted and maintained in a discontinuous way. Instead of leaving the trail along the whole route, the vehicles should generate a given amount of pheromones concentrated on a specific point of the road. That amount should be the equivalent to the pheromones emitted during a bounded path. In this way, the vehicles detect the trail of pheromones only in those specific points.

This modification requires preliminary planning to analyze the strategic points where to generate and detect pheromones.

C. Pheromones storage

The level of pheromones cannot be stored on the road, but in the vehicles for reasons of synchronization, as described in the next section. Hence, the proposed algorithm for traffic management is a distributed implementation of the algorithm used by ant colonies to find food.

III. Implementation Details

The algorithm presented in the previous section mainly relies on V2V communications. This resource allows the vehicles to send and receive messages representing the generation and detection of pheromones.

However, an auxiliary system is mandatory to manage the locations where the vehicles have to generate and/or detect the pheromones. In this paper, we consider two different proposals: RFID and GPS location. Next, this and other implementation aspects are described.

A. Location system

The radio frequency identification (RFID) systems have been outlined from the beginning as a way to extend the functionality of the Internet of Things (IoT) [2] to all kinds of objects, adding one tag with certain information that can be read and/or modified through a radio interface [9].

These systems basically consist of reader devices that interrogate some passive devices (tags), which respond by using energy they take from the field applied by the reader. Communication between the reader and the tag is established wirelessly by inductive coupling in the case of HF tags or backscattering in the case of UHF tags.

Since the communication between the tag and the reader is wireless and the tags do not need a power supply (they are passive), RFID system is a perfect candidate for our system. RFID provides I2V and V2I connections. Applications for toll control and automatic detection of traffic signs are supported by RFID [8],[13], [14].

Moreover, the Global Positioning System (GPS) is the most widely used location system based on satellite. At present, we can consider that the great majority of vehicles have a GPS signal receiver. In emergency situations, the vehicle may continue to use the system [16]. Therefore, it constitutes a good choice for the management system proposed in this paper.

In any case, RFID or GPS are necessary to establish the points of generation and detection of pheromones and route selection. These places are called control places.

B. Definition of control places.

The definition of control places is performed by means of the identification of the most significant nodes of the road. These nodes are the most important junctions or roundabouts. At each input, all possible outputs are considered.

Input locations are associated with locations where vehicles have to decide where to continue the route. To do so, the vehicles consult the data received from other vehicles. Output locations are used to indicate the vehicles when they must emit pheromones (Fig. 1). This emission consists of a message that primarily contains two values:

- ID_{SVeh} : Identification of the vehicle that caused the message
- ID_{loc} : Identification of the location that corresponds to the sending of the message

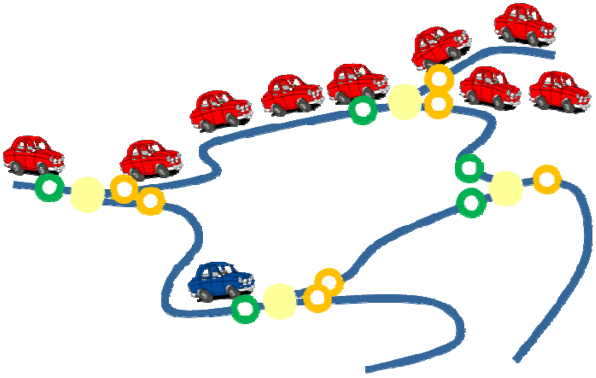

Figure 1. Identification of relevant places

C. *Vehicle configuration*

Pheromone levels generated by the vehicles are not stored on the road, as would ants, but kept updated in each vehicle independently. That is, each vehicle controls every pheromone emission produced in its area of interest.

To do so, vehicles use a register (internal local variable) for each output. We consider that, in this first stage of definition and prototyping, the vehicles know the control places before they begin to apply this system. In future stages, currently under work, we will consider that the control places will be dynamically discovered by the vehicles and incorporated to their internal maps.

The registers are initialized to zero. Each time a vehicle drives through a control place, a message that contains ID_{SVeh} and ID_{loc} is broadcasted, following the usual scheme employed in VANETS. When a vehicle receives a message, the register associated to ID_{loc} is updated.

Updating registers is not merely cumulative because we must take into account the effect of disappearance (evaporation) of pheromones in function of time. For this reason, it is essential to know the time between messages related to the same route.

This time control is locally (internally) performed. That is, the vehicles' clocks are not synchronized. The important thing is to know the arrival time difference of the messages related to the same route. Therefore, the vehicle will store the last timestamp received in each register.

D. *Pheromones generation*

Unlike ants, the vehicles generate pheromones at discrete points. In any case, the general behavior is very similar, in such a way that the generated pheromones are added to the existing quantity at every discrete point. At the same time, the accumulated amount of pheromones disappears as time passes. Hence, the generation and updating processes are as follows:

- **Generation process**. When a vehicle drives over a generation point, it sends a message with the identification number ID_{loc} of that location.
- **Disappearing effect**. When a vehicle drives over a generation point, it compares the timestamps of all registers with its current local time. In this way, the vehicle computes the time elapsed from the last pheromones generation. The time difference multiplied by a constant coefficient is applied to reduce the value of every register. Non-negatives values are not permitted.

  The rest of vehicles apply the same reducing algorithm when they receive the message. Each vehicle computes time differences and reduces the values of registers. Non-negatives values are not permitted.
- **Increase of pheromones**. Once the disappearing effect has been applied, every vehicle included the one that generates the pheromones, increases the register value in a constant quantity of 50. This value maybe modified. In the experiments performed 50 has resulted a suitable value.

E. *Route selection*

Each time a vehicle drives over a selection location, it performs the following operations:

- **Disappearing effect**. The procedure described in previous phase is applied to update the pheromones status of every decision node.
- **Selection**. The vehicle chooses the output road with the lowest level of pheromones. Actually, the vehicle only makes a recommendation. The driver chooses the output path following the recommendation. The driver could choose a different route. In any case, the final decision will be reflected on the system by means of pheromones generated when the vehicle drives over the route selected.

IV. Security Analysis

The ant algorithm has proven to be effective and ensures its adaptation to dynamic changes in the routes. This section discusses the security aspects of the proposed algorithm.

A. *General considerations.*

The proposed algorithm for traffic management is based on V2V message exchange through the VANET. Therefore, we should apply the same security mechanisms as other messages that are used to improve road safety. As described in [10] and [11], authentication is the main security mechanism to detect false messages. Confidentiality of information is not a priority because the main goal is to give maximum exposure while ensuring the authenticity of the same. Accordingly, the messages described in section III incorporate a signature to allow verification of the authenticity. The signatures are generated by means of asymmetric or identity-based cryptosystems.

Finally, since the algorithm of the ants has local significance, the life time of the messages must be small. That is, the number of hops should be limited in the routing protocol to a small value.

B. Reputation Lists and Data Aggregation

Authentication is the first barrier to prevent fraudulent messages. However, it is not enough since an authentic message can convey a false content devised by a user who wants to sabotage the system.

An attacker could try to overload a route sending false messages always indicating the same location, making believe that there are many vehicles on the road. In this way, the attacker would be reserving a path for himself, as other vehicles not choose a route congested.

In [11], reputation lists are proposed to identify vehicles that generate false content. Specifically, two types of lists were proposed: the individual reputation list (IRL) that internally updates each vehicle when it detects a fraudulent message, and global reputation list (GRL) that are shared with all vehicles with the help of some RSU. Messages generated by vehicles in one of these lists will be discarded and not retransmitted.

In this paper, we only use IRL because GRL rely on infrastructure and would not work in emergency situations. The IRL generation process is as follows:

- When a vehicle wants to emit pheromones sends a message containing its own identity ID_{SVeh} and its location ID_{loc}.
- Vehicles that receive the message check if ID_{SVeh} is in IRL. If so, then the message is discarded and not retransmitted.
- If ID_{SVeh} is not in the IRL, the vehicle checks whether ID_{loc} is consistent with their location, that is, that the message has been delivered from a nearby. Otherwise ID_{SVeh} is included in the IRL and the message is discarded and not retransmitted.

In a VANET, relaying messages cannot always be done at the right time. When a vehicle is not close to another vehicle, it cannot communicate. In these cases, the usual mode of operation of VANETs is to store the message and broadcast it later when another vehicle is found. This behavior affects the IRL, as a vehicle that receives a delayed message will have a different (distant) location, from which the message was originated, and therefore, will be considered as false.

To avoid this effect, this paper proposes aggregation of signatures as a method of message verification to complement the IRL. In [10], it is proposed the use of aggregation for warning messages on accidents and incidents affecting traffic safety. A vehicle that receives a message will add its signature only if it detects the same incident on the road.

This scheme is not applicable, as is, in the case of traffic management proposed in this paper. The ants algorithm only needs to send and receive messages containing the location of vehicles. Thus, vehicles can only detect if a message carrying ID_{loc} was sent from near or far to that location.

The combination of IRL and aggregation of signatures is performed as follows:

- When a vehicle wants to emit pheromones sends a message containing its own identity ID_{SVeh} and its location ID_{loc}. The message will be sent only if neighbor vehicles exist. Delayed messages will not be sent.
- Vehicles that receive the message check if ID_{SVeh} is in IRL. If so, then the message is discarded and not retransmitted.
- If ID_{SVeh} is not in IRL, the vehicle checks wether ID_{loc} is consistent with their location, that is, that the message has been delivered from a nearby. If so, the vehicle adds his signature to the message and retransmit it.
- If ID_{SVeh} is not in IRL, and ID_{loc} is not consistent with the current location, then if the message contains aggregated signatures, the message is accepted and retransmitted. Otherwise, ID_{SVeh} is included in the IRL and the message is discarded and not retransmitted.

C. Analysis of Possible Attacks

In a VANET, the main security threats come from fake content generation. An attacker could send messages indicating that is circulating in a location other than the one actually has, with intent to influence the overall perceived congestion on other vehicles.

In the particular case of the algorithm proposed, the security threats are less serious because it has implicit security. This means that the operation of the system itself makes attacker benefits are minimal.

Then we analyze security of the proposed system against possible attacks.

- **False messages**. They are detected by means of the usual authentication mechanism in VANETs.
- **False content** (fraudulent messages). They are detected by means of the combination of IRL and signature aggregation described in the previous subsection.

  In any case, if a false content escapes to the control of the proposed mechanisms, the implicit security of this traffic management algorithm minimizes the risk. So, if a vehicle sends a false content, the effect on the management system will be minimal, because if a single message gets to change the decision of other vehicles is because all the routes had a similar level of congestion. Equivalently, one could say that a single ant does not alter the behavior of the entire colony.
- **False content flooding**. Since a single message can not affect the rest of the vehicles, an attacker could generate a large number of fake messages containing the same location to achieve his goal. The procedure based on IRL and signature aggregation detects these fake messages. Furthermore, in the case that the procedure does not work properly, the situation is easily detected because the vehicles receive

messages with the same ID_{loc} and ID_{SVeh} in a short period of time. If the attacker decided to space in time the messages, then the success probability would decrease due to the effect of the disappearance of the accumulated pheromones.

- **Conspiracy**. A large number of attackers may collude to send messages with the same but different ID_{SVeh} ID_{loc}. If the messages are false, the IRL in combination with signature aggregation detect them. If this mechanism does not work properly, this type of attack is not the most efficient because it needs a large number of organized attackers to book the same route. They themselves would collapse the route.
- **Discarding an aggregate message**. The attacker will not retransmit the authentic messages, with the intention to perform a denial of service. This attack is not efficient. If the vehicle density is low, then the message will not be retransmitted but the influence on the traffic control will be negligible. If the density is high, there is a very high probability that another vehicle retransmit it.

V. PROTOTYPE

The model proposed in the previous section has been implemented as a scale prototype with two major objectives in mind: to broadcast the advantages of VANETs, and to provide a demonstrator platform where the effects on traffic management can be easily perceived. In this sense, we have chosen a real scenario determined by the road paths between two major hospitals at Málaga city, Spain.

The prototype is composed of one road circuit, several robotic vehicles, and a monitorization system. The communications between the actors are performed by means of RFID tags and readers and ZigBee modules.

A. *Test road circuit*

The road circuit has been printed on a 150 x 90 cm paper size. The dimensions are determined by the maximum width of the print area of the available printer device (90 cm), the size of vehicles and a value of length allowing to handle the prototype.

The road circuit has been previously designed using Microsoft Office Visio 2007 paying attention not only to the particular road paths to test, but also to aesthetic criteria in order to enhance the visual effect. Different road circuits, following the same guidelines, have been previously used to demonstrate the performance of other VANET functionalities [13].

The printed road circuit used in this protocol corresponds to a simplification of a real scenario located in Málaga city (Spain) between two major hospitals, "Carlos Haya" University Regional Hospital and "Virgen de la Victoria" University Clinical Hospital. Fig 2 shows the real map. Fig 3 shows the simplification that contains only the main avenues and streets, but maintaining the traffic senses. The circuit includes six decision nodes, marked with colors.

On the other hand, as one can see in Fig 3, the road is printed in white color (90 mm width) with a centered black line (20 mm width) to help the vehicles in the auto-drive functionality.

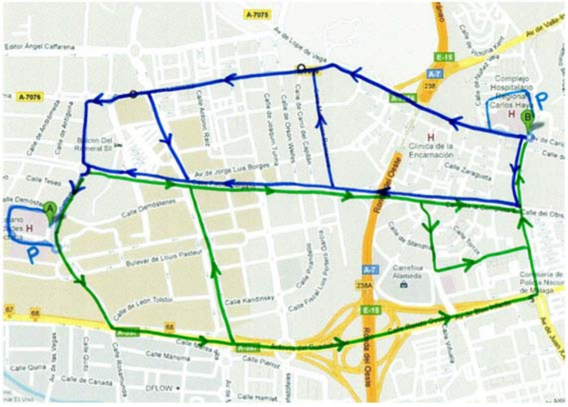

Figure 2. Real scenario (source: Google Maps)

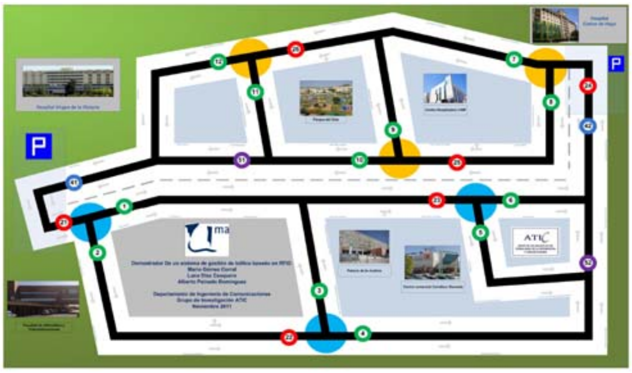

Figure 3. Prototype test road

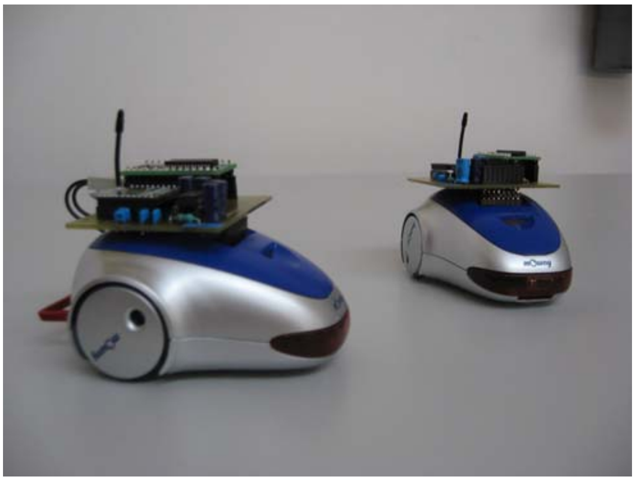

Figure 4. Robotic vehicles

B. *Robotic Vehicles*

The vehicles are little size robots with the ability to track a black line. This functionality is governed by a main PIC microcontroller and a secondary microcontroller dedicated to control the wheels movements.

The vehicles have been constructed using the educational Moway mini-robot as the starting point [12]. An additional PCB with an RFID reader and a Zigbee transceiver has been designed, developed and incorporated to every robot. Finally, the RFID antenna has been integrated in the own robotic vehicle (see Fig 4).

The robotic vehicles have been programmed to read the RFID tags located at the road and send and receive information over the ZigBee interface.

C. *Wireless communications*

The communication between the road and the vehicles is implemented by means of RFID technology. Read-only EM4100 passive tags operating at 125 kHz are located in the middle of lanes near the decision nodes. The vehicles are provided with the SM125-M1 RFID reader module by *SonMicro Electronics*.

V2V communications are implemented over a ZigBee interface. ZigBee is used, instead of another wireless technology, due to the reduced size of the prototype elements. Each vehicle is provided with a XBee module by *Digi International, Inc.* This module allows the vehicles the reception and transmission of pheromones.

The same Xbee module has been employed to develop an infrastructure point, in such a way that V2I communications could be performed. Actually, the model proposed in this work does not need the support of any infrastructure. However, the monitorization system, developed as part of the prototype, uses this service to obtain the status information from the circuit.

Finally, I2V communications are not implemented because the monitorization system does not return any information to the vehicles.

VI. CONCLUSIONS

We have proposed an algorithm, based on ant colonies, for road traffic management. The implementation of the algorithm does not rely on fixed infrastructures in order to operate in emergency situations. It only uses the VANET V2V communications and location systems that do not require contact with a fixed infrastructure.

The algorithm uses signature aggregation and reputation lists to ensure system security. Furthermore, the algorithm has an implicit security that minimizes the risks in case of attacks.

A scale prototype has been designed and implemented to validate the algorithm using RFID location system.

However, this proposal needs further work to optimize some configuration parameters and perform simulations to provide data about the final distribution of congestion.

Currently, identification of the locations is static. At a later stage, we will consider the integration of the proposal with dynamic maps, without prior planning. However, the current static solution is completely valid for emergency situations.

ACKNOWLEDGMENT

This work was partially supported by Ministry of Science and Innovation under Project TIN2011-25452 ("TUERI: Technologies for secUre and Efficient wiReless networks within the Internet of things with applications in transport and logistics") and by Universidad de Málaga. Campus de Excelencia Internacional Andalucía Tech.

REFERENCES

[1] Asset-road Project, 2010, http://www.project-asset.com [retrieved: June, 2013]

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, 2010, vol. 54, p. 2787-2805.

[3] E. S. Davison, H. Shmizu, and H. Naraki, “Traffic Signal control algorithms of a traffic network”, Proc. of IFAC Symposium Large Scale Systems, LSS’95, London, 1995, pp. 509-514.

[4] Y. Fang and L.B. Wu, "Parallel Ant Colony Algorithm for the Logistics Scheduling Problem”, International Conference on Multimedia Communications (Mediacom), Aug. 2010, pp.116-119.

[5] A. Gutiérrez Martín and F. Monasterio-Huelin, "Algoritmos de rastreo inspirados en colonias de hormigas", Actas de las XXVII Jornadas de Automática, 2006, pp 299-305.

[6] H. Hartenstein, VANET: vehicular applications and inter-networking technologies, John Wiley & sons, 2009.

[7] IEEE 802.11p, “Draft standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements: Wireless access in vehicular environments.” IEEE P802.11p/D9.0, September 2009.

[8] Y.M. Lee, C.G. Yoo, M. Park, M. Kim, and M. Gerla, “Installation and Evaluation of RFID readers on Moving Vehicles”, in Proc. of the sixth ACM international workshop on VehiculAr InterNETworking,VANET’09, 2009, pp. 99-108.

[9] S.B. Miles, S.E. Sarma, J.R. Williams, RFID. Technology and applications, Cambridge University Press, 2008.

[10] J.Molina, P.Caballero, and C.Caballero, “Data Aggregation for Information Authentication in VANETs”, Information Assurance and Security Letters, 1, 2010, pp. 47-52.

[11] J. Molina, C. Caballero, and P.Caballero, “Reputation Lists and Groups to Promote Cooperation”, International conference on Computer Systems and Technologies, CompSysTech’11, 2011, pp. 460-465, Vienna, Austria.

[12] Moway mini-robot. http://moway-robot.com [retrieved: June, 2013]

[13] J. Munilla, A. Ortiz, and A. Peinado, "Robotic vehicles to simulate RFID-based vehicular ad hoc networks", Proc 3rd International ICST Conference on Simulation Tools and Techniques (SIMUTools 2010), Torremolinos, Málaga, Spain, 2010, pp. 49,1-49,2.

[14] A. Ortiz, A. Peinado, and J. Munilla, “A Scaled Test Bench for Vanets using RFID Signalling”. in Comp. Intelligence in Security for Information Systems, 2009

[15] Roughan and O’Donovan – AECOM Alliance, Goodbody Economic Consultants, NRA National Roads Traffic Management Study, National Roads Authority Publications, Ireland 2011

[16] S. E. Shladover and S. K. Tan, “Analysis of vehicle positioning accuracy requirements for communication-based cooperative collision warning”, J. Intell. Transp. Syst., Technol., Plan., Oper., vol. 10, no. 3, 2006, pp. 131–140.

[17] D. Xiao-Hua Yu, "Traffic signal optimization using Ant Colony Algorithm", Neural Networks (IJCNN), The 2012 International Joint Conference on , June 2012, pp.1-7, 10-15.