

Security in VANETs: Lightweight Protocol for Group-of-Vehicles Masters (LPGVM)

Hamaciré El Hadj Kalil*, Ahmed Dooguy Kora* and Selma Boumerdassi†

*ESMT/eINNOV, Ex Terrain Foyer Rocade Fann Bel Air, BP 10 000 Dakar Liberté SENEGAL

†CNAM/CEDRIC, 292 rue Saint Martin, 75003 Paris, France.

elhadjalalpha@gmail.com, ahmed.kora@esmt.sn, selma.boumerdassi@inria.fr

Abstract – this paper focuses on the Vehicle Ad-hoc NETWORK (VANET), especially on the security of information exchanged in the network. We therefore propose in this document a secure communication protocol, based on VANET network standards. A lot of research is under way to make possible the large-scale deployment of VANETs. It is with this idea that we decided to propose a communication protocol based on an architecture organized in groups. For each group of vehicles, a Master is appointed who is the leader of the group. In our proposal, only a group Master can communicate with an RSU (Roadside Unit). In the literature, in general, the group leader takes care alone of managing the group. Here we involve the RSU in the group management to reduce the workload of the Master. In general, the organization of the group network lighten the workload of the RSU. But our proposal will also reduce the burden of the Master and thus significantly improve the performance of the network.

Keywords: VANET, Security, Protocol, Group, Master.

I. INTRODUCTION

Technological advances have led to the development of the Intelligent Transport System (ITS) [1]. To ensure the safety of people and provide an adequate logistic transport framework, the STI needs a dedicated communication network and disregards existing mobile networks. The concept of VANET networks was created in response to this need. VANETs bear a closer resemblance to MANET networks (Mobile Ad-hoc NETWORK). However, unlike MANETs, the nodes in a VANET have a very high mobility and thus the topology of the network changes constantly. Its architecture is composed of OBU (On-Board Unit), RSU (Road Side Unit) and TA (Truth Authority).

VANETs are a communication network in which the main nodes that interact are vehicles. They essentially allow to have two models of communication: the model vehicle to vehicle (V2V) direct communication between two vehicles; the vehicle-to-infrastructure model (V2I) communication between a vehicle and an infrastructure located along a road [1], [2], [3] and possibly a hybrid communication [4] combining the two models.

The main objective of VANETs is to ensure the safety of road users by considerably reducing road accidents [1]. Through the dissemination of information, alerts and warnings, technical assistance in case of accident and criminal investigation [5], VANETs create a safer environment for road traffic. In addition

to security applications, VANET also offers applications for passenger entertainment, toll management, on-board commerce [5] and so on.

However, to enable the popularization of VANETs and to take full advantage of these many features they offer, it is necessary to have secure communication protocols and having such protocols is one of the many challenges faced by researchers. The difficulty of secure communication protocol design lies in the mobility of nodes that often move at high speed, the frequent change in network topology and the end-to-end message transmission time that must be less than 150 ms [3].

VANETs are similar to MANETs therefore they inherit security issues related to the radio interface experienced by MANETs, such as malicious attacks. The security protocols must therefore take into account the basic security requirements defined in [6] to be able to fight against malicious attacks. They also need to address latency and data loss issues, due to the amount of data that nodes must handle if the architecture is not well conceived and may have a negative impact on network security and performance [7].

In VANET the transmission delay is very important, so we need a short delay and because of this the connections between vehicles must be the most efficient possible. That's why in our solution, the Master of a group is chosen to have the best signal with the RSU and each vehicle chooses the Master which offers him the best signal to join his group. Thus we increase the chances of availability of the connection within the network on the one hand and within each group on the other hand and finally we will be able to guarantee the delay.

It is within this framework that we define the objective of this work, which is to propose a secure communication protocol based on an architecture organized into vehicle groups. The protocol makes it possible to lighten the load of the Group Master by involving the RSU in managing the groups and to offer the network a transmission delay that complies with the standards.

In this document we adopt the following approach: after the state of the art in II, we propose a secure communication protocol in III, then a discussion on the contributions of this protocol and comparison with the protocol defined in [8] in IV before concluding.

II. THE STATE OF THE ART

A. Standards

The standard architecture of VANET is composed of three essential elements [1], [3] which constitute the very foundation of the VANETs. These components are:

- OBU (On-Board Unit) a tamper-proof device [1] installed in the vehicle and which allows them to communicate with the nodes of the network,
- Roadside Unit (RSU), also known as Roadside Infrastructure, is a roadside relay antenna that provides V2I communications,
- TA (Truth Authority) a certification center that issues vehicle identifiers and authenticates each vehicle before it enters the network.

According to [9], in 1999 the FCC allocated a spectrum of 75 MHz in the 5.9 GHz band [3], [10], [11] for DSRC (Dedicated Short-Range Communications). DSRCs are short-range, unidirectional or bidirectional wireless communications specifically designed for the Intelligent Transportation System (ITS). DSRC supports the V2V and V2I communication models of VANETs.

The 75 MHz spectrum allocated to DSRCs has been planned to offer 7 channels of 10 MHz bandwidth each. One of these channels is reserved for security communications (CCH: Control Channel) and the two channels at the edge of the spectrum are reserved for specific purposes. The rest of the channels (SCH: Channel Service) are used for the different services.

According to [9], [12] VANET uses the IEEE-802.16 standards (Wireless MAN / WIMAX) for multimedia applications and IEEE 802.11p for V2V and V2I communications [13].

B. Related works

Many works are carried out to provide security solutions in VANETs networks, including confidentiality, authentication and the topological or architectural structure of the networks. For VANET, the architecture that seems the most appropriate in the literature is the one in which vehicles are organized in groups.

For the future, in [8] the authors define another approach for group architecture. Here the group is created autonomously without the intervention of the RSU. Each group contains a CH leader and a GW gateway that provides intergroup communication. In this algorithm a vehicle may have the state UN (initial state), CHt (temporary group leader), CH (group leader) or CM (group member); the GW is a CM at the edge of the group.

In [3] the researchers demonstrated from the results of a simulation that the decoding computation time of the Chinese Remainder Theorem RSA algorithm (CRT-RSA) is faster than that of simple RSA. The proposed mechanism consists of three phases: registration of a vehicle, sending and receiving messages and leaving a group. In this mechanism each OBU can only communicate with the RSU and in turn broadcasts the information in the group. Indeed, each RSU and all the OBU under its cover constitute a single group whose leader is the RSU.

[4] defines an architecture in which groups are dynamically organized. When a group is formed, a GL (group leader) is appointed. The GL generates an asymmetrical group key pair that it shares with all members in an encrypted message the symmetrical key of the group. The new vehicle is authenticated by the RSU from which he obtains a certificate, an asymmetrical key and a symmetric key. And once it joins a group; he receives asymmetric and symmetrical keys of this group that he will now use to communicate within the group.

[13] defines a CH selection method based on the distance between vehicles and centroids. The Algorithm first establishes a list of eligible CHs according to their bandwidths. It then defines the number of groups initially possible; this number is equal to the number of centroids. And lastly, the eligible CHs closest to the centroids are defined as CH for the vehicles of their neighbors.

[14] proposes an architecture organized in a group whose CH is chosen according to three approaches. The first approach is based on the mobility, the direction and the density of the vehicle, the second approach is based on the distance between the RSU and the vehicle and the third approach is that based on connectivity with other vehicles.

[15] proposes a method of group formation based on the average speed of movement of vehicles and the number of neighbors of each vehicle. The vehicle with the speed closest to the average and the largest number of neighbors is chosen as the group head (CH). And to extend the life of the CH, the coverage radius of the group is defined according to the average speed and the vehicle density in the network.

[1] shows a secure communication technique of VANET based on a blind signature scheme. The algorithm used in this scheme is RSA and involves 3 entities for a communication, namely the initiator, the signatory and the recipient. A fourth entity is identified in the schema that is defined in [1], and it is the registration / revocation authority responsible for the blinding identity.

In [7] the authors propose an intersection system at the level of traffic lights through which vehicles can negotiate between each other the order of crossing at intersections or an intersection manager accepts vehicle requests and decides on the order of passage of the vehicles. In both cases the results are better than the ordinary management of traffic lights.

[16] proposes a randomized token protocol, called DBT-MAC, which depending on the simulation results offers better results than the IEEE - 802.11p standard. An anti-Sybil attack algorithm is defined in [17].

III. LPGVM PROTOCOL

A. Global idea

The protocol is based on the standard architecture defined in [1], [3] consisting of OBU, RSU and TA. However even if the architecture remains the same, for the operation of our protocol the vehicles will be organized in groups. A group contains a defined and limited number of vehicles. For each group a vehicle is designated by the RSU as Master and it is the latter who

communicates with the RSU. Like [4] and [8], in order to extend the life of the groups, they are composed of vehicles traveling in the same direction.

The V2V communication model is limited only within each group and between neighboring Masters and the V2I model between the Master of each group and the RSU. The Master creates a database in which he provides information about each member of the group and the neighboring Masters. As for the members, each one retains the information relative to the other members of his group and his Master.

Each node is characterized by a temporary identifier (IDtmp) and a certificate assigned to it by the trusted authority / certification (TA). For the continuation, we admit the following notations of the table I:

TABLE I. Meanings of certain acronyms

Notation	Signification
IDtmp	Temporary identifier of a vehicle
Cpu	Asymmetrical public key
H	Timestamp
Cgeo	Geographical coordinates of any entity
Cert	Certificate (to identify the vehicle when entering the network)
THT	Threshold Handover Time (a minimum time observed by a node before performing an action)

The overall architecture is defined by the following figure:

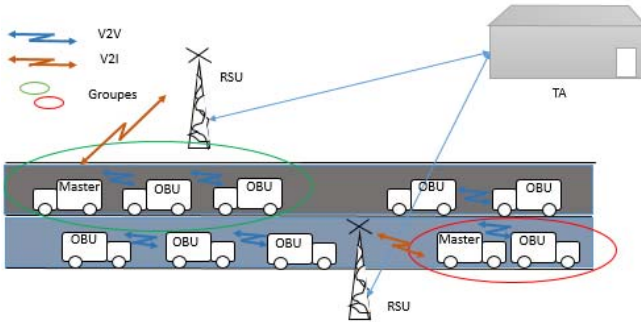


Figure 1. Global Architecture

B. Authentication of the nodes

Each node goes through an authentication procedure through the network each time it has to reconnect.

The call-flow of the authentication of the nodes is illustrated by FIG.

- (1) The RSU broadcasts a signed beacon signal containing its public key (C_{pu_rsu}), the timestamp (H_{rsu}) and its geographical coordinates (C_{geo_rsu}),
- (2) The OBU requests authentication by sending the RSU its certificate ($Cert_obu$), its public key (C_{pu_obu}) and the timestamp (H_obu) in an encrypted and signed message,

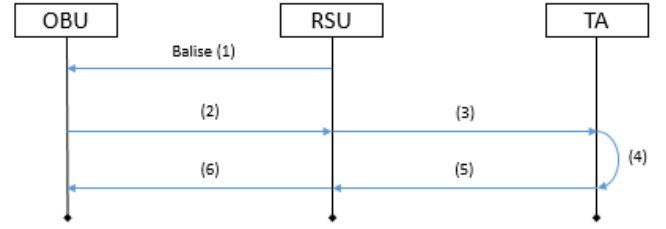


Figure 2. Call-Flow authentication

- (3) The RSU transfers the information to the TA to authenticate the OBU,
- (4) The TA verifies that the OBU is registered and validates its authentication,
- (5) The TA acknowledges the authentication by assigning to the OBU a temporary identification number (IDtmp),
- (6) The RSU sends the result to the OBU who may at this time request membership in a group.

C. Selection of the Master and creation of groups

As seen in the previous section, initially an offline vehicle that had just discovered the network must go through an authentication phase. An offline vehicle is a vehicle turned off, off-cover, new etc.

The RSU measures the signal reception quality of each connected vehicle and selects those with the best signal as potential masters. Then all those who respect the D_{min} condition are declared definitively, Group Masters, and at the same time the group is created through the assignment of a group ID. Once the Masters are named and the groups created, the other nodes can choose in turn a group according to the reception levels of the signals received from the different masters.

D. Fusion of groups

In our mechanism, we define a distance (D_{min}) the minimum distance which must separate two neighboring Masters, it is also the triggering element of the fusion of two groups. And we name (D_{xy}) the real distance that separates two neighboring Masters. Thus, the process of merging two groups is triggered when the distance (D_{xy}) becomes smaller than D_{min} for time (THT).

The group with the largest IDgroup is dissolved to be added to the group with the smallest IDgroup. The call-flow of fusion is the following one (we suppose that the condition $ID_{groupA} < ID_{groupB}$)

- (1) The MasterA sends the RSU a merging request message containing the two IDtmps of both groups,
- (2) The RSU checks if the same request is not already initiated by the MasterB, then compares the two IDtmp and identifies the largest,
- (3) The RSU, after processing, sends IDgroupA to the MasterB so that it can be ready to change its Master status. The MasterB disseminate the new IDgroupA to members of its group to change their group ID,

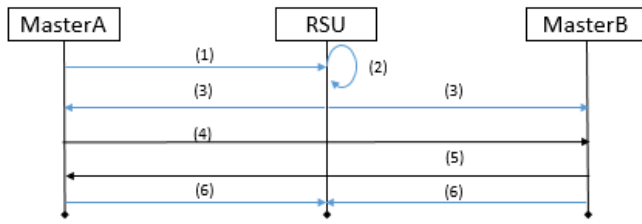


Figure 3. Call-Flow of fusion of two groups

- (4) The MasterA shares the list of its members with the MasterB so that the members of the group B can know the members of the new group that they must join,
- (5) The MasterB also shares the list of its members with the MasterA which in turn shares it with its members,
- (6) Both Masters acknowledge the process with the RSU, and thus group B is dissolved and both groups form a single group A.

NB: If the RSU does not receive phase (6) from one of the two Masters then it sends a cancellation command to both Masters and resumes the process from phase (3).

E. Masters Management

After choosing Masters and creating groups, each master organizes the members of his group by assigning each a position corresponding to the quality of his signal. Thus, members can have the denomination master2, master3..., mastersn. This classification always follows the law of the strongest signal to the main Master's position.

The Master can change status to a second rank when:

- its signal becomes lower than that of another node X and during a fixed time. At this moment the node X becomes Master and the old Master will occupy a lower rank corresponding to the level of its signal,
- it picks up a better signal from another RSU for a time (THT) and changes RSUs,
- he stops (off).

In the case that two nodes have the same signal level, the one with the lowest ID becomes Master. It is the RSU that takes care of changing the Master.

F. Join a group

All Masters continuously broadcast a beacon signal containing IDtmp, Cpu and timestamp (H) according to [1]. The following figure illustrates how a node can join a group.

- (1) The Master broadcasts its IDtmp, Cpu, H and its geographical coordinates (Cgeo) in a signed message,
- (2) The OBU sends to the Master its IDtmp, Cpu, Cgeo and H in an encrypted and signed message,
- (3) The OBU requests authentication of the Master from the RSU by sending it in an encrypted and signed message, the IDtmp and Cgeo of the Master,
- (4) The Master also sends the IDtmp and Cgeo from the OBU to the RSU for authentication in an encrypted and signed message,

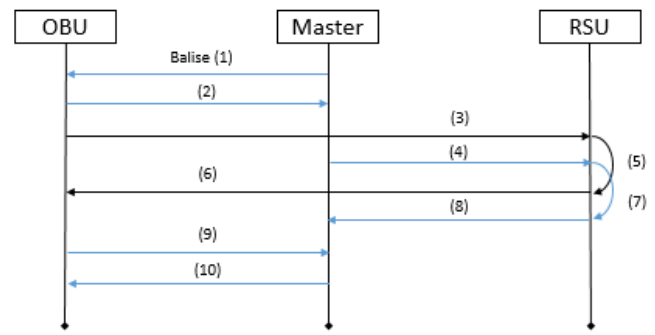


Figure 4. Call-Flow to join a group

- (5) The RSU processes the request of the OBU,
- (6) The RSU responds with an ACK message at the request of the OBU,
- (7) The RSU processes the request of the Master,
- (8) The RSU fulfills the request of the Master,
- (9) The OBU sends to the Master a request to join the group,
- (10) The Master accepts the membership application and shares the new member's credentials with other members to update their databases.

NB: if only one of the two nodes does not receive an acknowledgment from the RSU then the membership process is interrupted and blocked. Similarly, the process does not start if the group has already reached its limit.

G. Change of group or RSU

Each vehicle keeps a list of the signals it receives from different Masters in its surroundings. It arranges them in the order of the strongest signal to the weakest, the strongest being that of the current group to which it belongs. When a signal becomes stronger than that of its current group during THT, then the vehicle asks to leave its group to join the group from which it receives the strongest signal. To do this the OBU initiates the following flow (it is assumed that the vehicle is currently in group A):

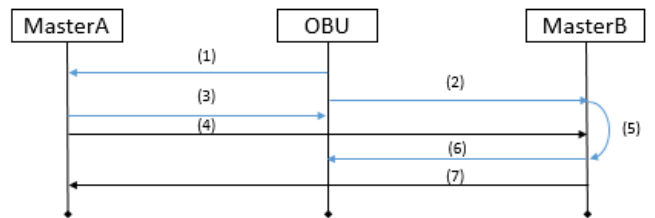


Figure 5. Call-Flow group change

- (1) The OBU sends a message to the MasterA to indicate the new group to which it wants to adhere, the message contains the IDtmp of the MasterB,
- (2) The OBU sends a message to the MasterB to request to join his group. The encrypted and signed message contains the IDtmp, the Cpu and the Cgeo,
- (3) The MasterA accepts the request of the OBU,

- (4) The MasterA sends the IDtmp to the MasterB to confirm the request of the OBU,
- (5) The MasterB compares the IDtmp received from the MasterA and that received from the OBU,
- (6) The MasterB accepts the membership request of the OBU and sends him the information of the group. The MasterB shares the arrival of the new member with the other members of the group so that they update their databases if the result of (5) is OK. It declines the request of the OBU if there is no matching during phase (5).
- (7) The MasterB informs the MasterA of the acceptance / rejection of the request of the OBU. The MasterA releases the OBU and asks other members to update their databases.

The process of change of RSU is done in the same way except that in place of Masters and OBU we will have RSUs and a Master respectively. Only a Master can initiate the RSU change process because an OBU automatically belongs to the same RSU as his Master.

NB: In the case that the group change process is successful, the OBU sends its new group ID to the RSU so that it updates itself.

IV. DISCUSSION

[4] and [8] define different but similar mechanisms to our proposal. We have therefore performed in the following table (Tab. II), a comparison of the three mechanisms.

The election of the Masters and the creation of the groups are carried out by the RSU, the management of the groups is shared between the RSU and the Masters. This mechanism makes the Masters less busy than the CH and GL who must create and maintain the groups: merging and changing of group, periodic calculation of parameters, changing of keys every 5 minutes. As a result, packets loss is less likely to happen at the Masters levels.

TABLE II. Comparison of the three mechanisms

Element	Our proposition	Proposition [8]	Proposition [4]
Group leader	Master	CH	GL
Communication model	V2V & V2I	V2V	V2V & V2I
Intra-group communication	Each member can diffuse within the group	Only the Chief diffuses within the group	Each new member diffuses beacons in his neighborhood of which each partisan measures the reliability of the new one and sends the result to its leader
Intergroup communication	$CHEFi \rightarrow CHEFj$; $CHEFi \rightarrow RSU \rightarrow CHEFj$	$CHEFi \rightarrow GWi \rightarrow CHEFj$; $MBREi \rightarrow CHEFi \rightarrow GWi \rightarrow CHEFj$	The CHEF (GL) only can broadcast the CRL certificate revocation list to neighboring groups; Vehicles in overlapping groups provide multi-hop communication.
Messages number	One message per information within the same group	One to two messages per information within the same group	One to two messages per CRL information within the same group
Databases (DB)	Each member creates a DB containing IDtmp, Cpu of each member of the group, possibly neighboring Masters for the case of the Master and the IDgroup	Only the group leader creates a DB containing the group information	Each member creates a DB listing the level of reliability (honest, intermediate and malicious) of neighboring vehicles.
Groups creation and management	RSU	Autonomous	Dynamic
Group merging	YES, based on distance	YES, based on distance	NO
Group merging condition	Based on the distance between two neighboring Masters	Based on two neighboring groups' overlapping	NO
Leaders Processing Charge	Dissemination of messages within the group, transmission to other leaders and RSU	Message broadcasting within the group, distance calculation with each member, choice of GW	Periodic calculation of the confidence of the new vehicles and classification of the members in order of security level; transfer of the CRL at each passage through a RSU; CRL dissemination to neighboring groups
Datas loss	Less risk of overflow and therefore less data loss	Saturation more likely therefore risk of data loss	More charge therefore more likely saturation and consequently packet loss
Conflict management	Based on IDtmp	Based on distance	NO
Choice / Position of the group leader	Having the best signal received from the RSU within the group	Having the central position in relation to the other members of the group	Having the highest level of reliability

V. CONCLUSION AND PERSPECTIVES

We propose a secure communication protocol allowing the authentication of the nodes at the entrance of the network, the change of group / RSU, the fusion of group and which lowers the workload of the Masters thanks to the maintenance shared with the RSU and the creation of groups that is reserved for the RSU. The protocol is based on an organized vehicle group architecture and supports intragroup communications, intergroup communications and group merging. Both V2V and V2I communication models are also supported in exchanges.

This protocol could be strengthened in future work. In our perspectives, we study the support for detecting abnormal behavior of vehicles that are already authenticated but that have suspicious behavior and the parameters that allow the protocol to be able to learn from the information collected in the network and to adapt to different behaviors that may occur in the network.

REFERENCES

- [1] Esti Rahmawati Agustina, Arif Rahman Hakim, *Secure VANET Protocol using Hierarchical Pseudonyms with Blind Signature*, 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok - Indonesia, 26-27 octobre 2017, IEEE, pp 1-3
- [2] Lina Bariah, Dina Shehata, Ehab Salahat and Chan Yeob Yeun, *Recent Advances in VANET Security: A Survey*, 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston - MA, USA, 6-9 septembre 2015, pp 1
- [3] Islam Z. Ahmed, Taha M. Mohamed, Rowayda A. Sadek, *A Low Computation Message Delivery and Authentication VANET Protocol*, 2017 12th International Conference on Computer Engineering and Systems (ICCES), Cairo - Egypt, 19-20 décembre 2017, pp 204-207
- [4] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis Laouiti, *A Security Solution for V2V Communication within VANETs*, 2018 Wireless Days (WD) Dubai, United Arab Emirates 3-5 avril 2018, IEEE, pp 181-182
- [5] Akash Vaibhava, Dilendra Shuklab, Sanjoy Dasc, Subrata Sahanad, Prashant Johri, *Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey*, International Journal of Wireless and Microwave Technologies May 2017, RESEARCHGATE, pp 41-42
- [6] Rajdeep Kaur, Tejinder Pal Singh, Vinayak Khajuria, *Security Issues in Vehicular Ad-hoc Network (VANET)*, 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli - India, 11-12 mai 2018, IEEE, pp 885-886
- [7] Bowen Zheng, Muhammed O. Sayin, Chung-Wei Lin, Shinichi Shiraishi, Qi Zhu, *Timing and Security Analysis of VANET-based Intelligent Transportation Systems*, 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine - CA, USA, 13-16 novembre 2017, pp 984, 986-988
- [8] Mengying Ren, Lyes Khokhi, Houda Labiod, Jun Zhang, Veronique Veque, *A new mobility-based clustering algorithm for Vehicular Ad Hoc Networks (VANETs)*, NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul - Turkey, 25-29 avril 2016, pp 1204-1206
- [9] Salim Bitam, Abdelhamid Mellouk, Sherali Zeadally, *Bio-Inspired Routing Algorithms Survey for Vehicular Ad-hoc Networks*, Published in IEEE Communications Surveys & Tutorials on 26 novembre 2014, pp 5
- [10] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, Woong Cho, *A Security and Privacy Review of VANETs*, Published in IEEE Transactions on Intelligent Transportation Systems on 17 juin 2015, pp 2986
- [11] M.J. Booyens, S. Zeadally, G.-J. van Rooyen, *Survey of media access control protocols for vehicular ad hoc networks*, Published in IET Communications on 01 aout 2011, IEEE, pp 1623
- [12] Rashmi Mishra, Akhilesh Singh, Rakesh Kumar, *VANET Security: Issues, Challenges and Solutions*, 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai - India, 3-5 novembre 2016, pp 1051
- [13] Rong Chai, Xianlei Ge, Qianbin Chen, *Adaptive K-Harmonic Means Clustering Algorithm for VANETs*, 2014 14th International Symposium on Communications and Information Technologies (ISCIT), Incheon - South Korea, 24-26 septembre 2014, pp 234, 235
- [14] A.v. Sutagundar, Pampapati Hubballi, Ravikant Belagali, *Stability Oriented Cluster Dynamism in VANET (SOCDV)*, IEEE, 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore - India, 6-8 Oct. 2016, pp 117 - 119
- [15] Anita Bavalatti, Ashok V. Sutagundar, *Multi-Agent Based Stable Clustering In VANET*, IEEE, 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), Bangalore - India, 17-19 Aug. 2017, pp 1034 - 1035
- [16] Ali Balador, Annette Bohm, Carlos T. Calafate, Juan-Carlos Cano, *A Reliable Token-Based MAC Protocol for V2V Communication in Urban VANET*, IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia - Spain, 4-8 septembre 2016, pp 2-4
- [17] Chen Chen, Xin Wang, Weili Han, Binyu Zang, *A Robust Detection of the Sybil Attack in Urban VANETs*, 2009 29th IEEE International Conference on Distributed Computing Systems Workshops, Montreal, QC, Canada, 22-26 juin 2009, pp 272-273

Hamaciré E. KALIL is graduated in ICT Engineering in 2017 from "Ecole Supérieure Multinationale des Télécommunications" (ESMT), Dakar - Sénégal. Currently, he is Ph.D student at ESMT and IT Consultant at Talents Consulting, Dakar - Senegal. His research area cover VANET, Telecoms, SoftWare development etc.



Ahmed D. KORA is IEEE senior member. He is graduated in ICT Engineering in 2003 from "Ecole Supérieure Multinationale de Telecommunications" (ESMT), Dakar, SENEGAL. He received his Ph.D. degree in telecommunication from the University of Limoges, France, in 2007. He is promoted as full professor by the regional accreditation institution (CAMES) and currently the Director of Teaching, Trainings and Research at ESMT. His research area covers QoS/QoE, network radio coverage, fiber optic transmission system, communication and networks system architecture, open network management solutions, universal access, low cost IT systems for development, etc.



Selma Boumerdassi is an Associate Professor at Conservatoire National des Arts et Me'tiers, Paris. She received a Ph.D. in Computer Science from University of Versailles in 1998, where she also served as an Assistant Professor from 1998 to 2000. Her research interests include wireless and mobile networks, with a special focus on the impact and use of social networks. Selma Boumerdassi worked on several national projects and served as an expert for the evaluation of French national projects (ANR). She is the author of more than 50 articles and serves as a TPC member for various international journals and conference

