SOTM: A SELF ORGANIZED TRUST MANAGEMENT SYSTEM FOR VANET

Amel Ltifi[1], Ahmed Zouinkhi[2] and Mohamed Salim Bouhlel[1]

[1]Research Unit: Sciences and Technologies of Image and Telecommunications, Higher Institute of Biotechnology of Sfax-Tunisia
altifi@gmail.com
[2]Research Unit: Modeling, Analysis and Control of Systems, National Engineering school of Gabes-Tunisia
Ahmed.zouinkhi@gmail.com

ABSTRACT

Security and trust management in Vehicular Adhoc NETworks (VANET) is a crucial research domain which is the scope of many researches and domains. Although, the majority of the proposed trust management systems for VANET are based on specific road infrastructure, which may not be present in all the roads. Therefore, road security should be managed by vehicles themselves. In this paper, we propose a new Self Organized Trust Management system (SOTM). This system has the responsibility to cut with the spread of false warnings in the network through four principal components: cooperation, trust management, communication and security.

KEYWORDS

Active vehicle, cooperation , trust management, VANET

1. INTRODUCTION

Road safety is the purpose of many researches and projects over the world, given the huge number of deaths and accidents [1]. VANET is a subclass of Mobile Ad-hoc Networks aiming at enabling a set of services for vehicles such as road security. It's a set of vehicles. Each one can communicate with other vehicles using DSRC (Dedicated Short Range Communication) technology (5.9 GHz) that supports ranges of up to 1 KM [2]. The vehicle is equipped with an On Board Unit (OBU). Each OBU is composed of a Global Positioning System (GPS) receiver, an Event Data Recorder (EDR), front radar, rear radar and a central computing system. EDR archives the sent/received messages to be available for use in emergency states. GPS receiver lends information about location, direction, speed and acceleration of the vehicle at a specific time. The computing system is used for data processing. Currently, VANET is the principal element in most current suggestions aimed at enhancing driving conditions. Intelligence ambient (AmI) and ubiquitous computing are new challenging technologies that can be used among VANET applications [3]. The concept of active object is a principal element in the AmI technology. It's recently introduced as an element of the active security in critical domains such as chemical industry [4].

David C. Wyld et al. (Eds) : NETCOM, NCS, WiMoNe, CSEIT, SPM - 2015
pp. 69–81, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.51607

This paper illustrates a self organized trust management scheme for VANET. The nodes of this network are Active vehicles which can communicate with each other, they can decide about trustworthiness of received alerts messages, and they can manage their security states.

The organization of the paper is as follow: after an introduction, the second part presents some related works. The third part presents components of the proposed system SOTM. We dedicated the forth part for model evaluation. Finally, the fifth part concludes the paper.

2. RELATED WORK

Only a few trust models have recently been proposed for enhancement reliable information spreading in VANETs. For example, authors in [5], [6] have investigated in security and privacy on trust establishment in VANETs that relies on a security infrastructure and most often makes use of certificates. A survey on this kind of trust models can be found in [7]. Another different class of trust models is a set of systems which are independent from static infrastructure. In these models, cooperation between vehicles is the key to determine the trustworthiness of data transmitted between peers.

Golle et al. [8] present a technique that aims at addressing the problem of detecting and correcting malicious data in VANETs. Each vehicle maintains a model of VANET that contains all the knowledge that a particular vehicle has about the network. Data evaluation is done according to its coincidence to the peer's model of VANET.

A sociological trust model is proposed in [9] based on the principle of trust and confidence tagging. A new architecture for securing vehicular communication and a model for preserving location privacy of the vehicle are presented.

Dynamic Trust-Token (DTT) is an approach to strengthen cooperation in VANET [10]. The purpose of this mechanism is to detect and prevent misbehavior nodes intervention in the transmission of packets, and ensure the integrity of packets over the releases. DTT uses two cryptographic mechanisms: symmetric and asymmetric, to protect the integrity of packages. Thus, it applies "Neighborhood WatchDog" [11] to generate the trust token that based on instantaneous performance to verify the correctness of packets. Thus, many different solutions that rely on existing historical reputation or past records, DTT is based only on execution performance to implement instant reputation for each node, where no accumulation of information is necessary. With DTT, the packets containing incorrect information will not be propagated in VANET. In this approach, each node can play three logic roles: Predecessor, Relaying and successor in the process of transmission of the packet over time.

In our work, we established a trust management system based only on cooperation between vehicles. This work provides a new communication protocol between vehicles to be able to differentiate between trusted and non trusted messages transmitted in VANET.

3. SELF ORGANIZED TRUST MANAGEMENT SCHEME (SOTM)

The proposed scheme is based on the interaction and the communication between active vehicles supposed to manage by themselves their own security states. For this purpose, we have introduced the concept of active vehicle as a result of the integration of the ambient intelligence

in the intelligent transport technologies. A new protocol of communication is defined between vehicles based on messages exchanging and aiming to have the ability to each vehicle to decide if a warning message received is correct or not. The SOTM system is composed of four principal components as depicted in figure 1. In this section, we will explain the roles of these four components.

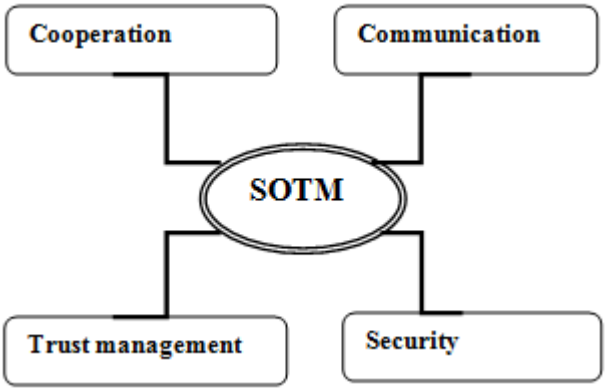

Fig.1 Component-based architecture for SOTM

3.1. Communication module

Generally, peers in VANET can communicate according to three modes of communication: Vehicle-to-Vehicle (V2V) among vehicles, Vehicle-to-Infrastructure (V2I), between vehicles and Road-Side Units (RSUs), and Vehicle-to-X (V2X), mixed V2V-V2I approach. In SOTM, vehicles are allowed to communicate only with V2V mode. For emergency message routing, the clustering model is applied. For each community of vehicles, there is a group leader that has the role of a trusted authority. There are two types of links between vehicles as depicted in figure 2: Unicast link and broadcast link.

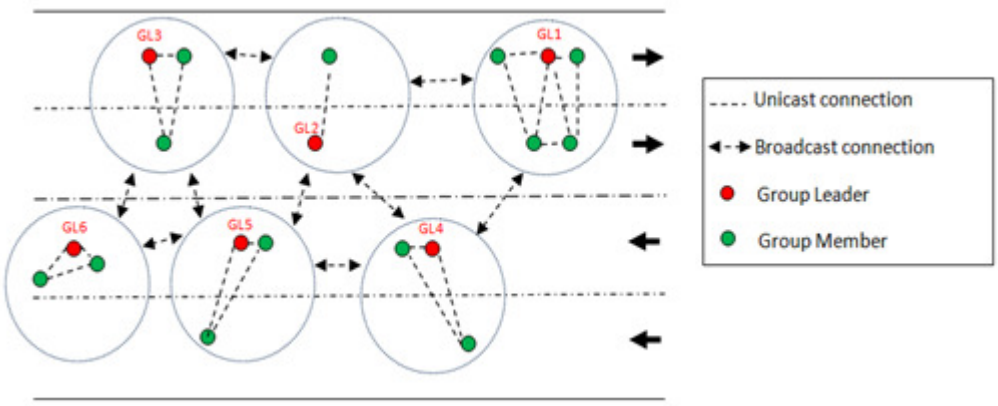

Fig.2 connection model between vehicles

This kind of application is very close to ad-hoc networks. In this situation, vehicles manage by themselves the traffic state. The V2V uses the standard IEEE 802.11p specification for network connection [12]. The 802.11p is an approved variant of the standard 802.11 used for Wi-Fi. The used band of spectrum is between 5.85GHz and 5.925GHz.

The vehicle-to-vehicle communication can be used alone on account of the existence of new wireless technologies and especially the IEEE 802.11p standard. The inter-vehicular communication gains benefit from wireless ad-hoc Networks and GPS to guarantee stable one hop and multi hop communications between vehicles [13].

Routing algorithm is the mainly challenging mission for VANET because of the strict requirements of VANET to high speed mobility and a rapidly changing topology [14]. For this reason, we opted to use a clustered architecture to create a network vision more stable and more reduced to each vehicle [15].

3.2 Trust management model

The aim of our work is to create a community of vehicles that is able to manage by itself its own active security state. It relies on the presence of communicant vehicles on the road. Each vehicle plays a specific role as a member of a disciplined community. To train vehicles facing their active security states, a new communication strategy is deployed by our trust management model. A set of rules is defined and should be applied concerning the collaboration way between vehicles. A knowledge base system is defined in the SOTM system to be integrated in the vehicle to be able to decide on received alarm messages trustworthiness.

3.2.1 Vehicles tasks in SOTM system

VANET is a sub-class of Ad-hoc networks. In such an environment, the trusted authorities couldn't be a part in the majority of security systems. In our case, the disciplined communication between vehicles is the key to create a stable community of vehicles that offers a number of services of road security. There are three main tasks for an Active Vehicle: announcement, communication and revocation. We will present in this part a description and the exchanged messages in each state.

3.2.1.1 Task 1: the announcement

During its driving life time, the vehicle may pass through different groups or it may create a new group. In order to announce its coming into a group, it should send a HELLO message on broadcast. The group leader GL should send an acknowledgement to the new coming vehicle that saves the address of the GL to be used during its transit through this group.

The "HELLO" message contains two fields. The first field is the identifier of the message sender. The vehicle identifier is a unique number aimed to distinguish between vehicles. And the second field is the public key generated by the On Board Unit (OBU) of the vehicle to be saved by the leader. We used the RSA method to achieve the authenticity and the integrity of messages. The "AckHello" has one field which is the leader Identifier.

3.2.1.2 Task 2: the communication

As is the case of any person in a human society, an active vehicle couldn't manage its security state without the interaction with other vehicles. It cooperates with its neighbourhood to be informed if there is an accident in the same space to react quickly. It should also transmit the received emergency messages to others. Before reacting and transmitting warning messages, the active vehicle should be sure about the trustworthiness of the received message. There is a set of messages exchanged between vehicles during their communication.

The “GRE” message is a periodic message sent by each vehicle member after the announcement step. It contains its type and the Id of the sender.

The “WARNING” message is sent by a vehicle when it detects an accident or an obstacle on the road. The destination of this message is the leader that verifies the trust level of the sender to decide whether to accept it or to ignore it. In the case of acceptance, first, the leader remunerates the sender by incrementing its Cooperation Counter, and second, it sends an “AckWARNING” to the sender to allow to it to transmit the warning to its successor. This message contains two fields: The Id of the sender and the warning number (numWrg) which is a unique number affected to each warning by the leader to distinguish between different warnings transmission sessions. A warning transmission session begins when the vehicle which triggered the warning receives an “AckWARNING” message from the leader. Consequently, it sends an “ALARM” message to its successor (the closest neighbor). The “ALARM” message contains the Id of the sender, the signature of the sender computed by its OBU based on the hashing method SHA-1 and the Data field containing the warning message.

When the vehicle successor receives the “ALARM” message, it should decide whether the warning is true or false. So, it begins the verification procedure by sending a “CONFIRM” message to the group leader to verify the trustworthiness of the sender. In this case, there are three possible statements:

• State 1: The sender is trustworthy. So, the leader sends a “VALIDATION” message to the vehicle successor to be able to transmit the “ALARM” message to another successor. The “VALIDATION” message contains the Id of the sender (IdS), the public key (KeyPb) used to verify the authentication of the sender and the warning number (NumWrg).

• State 2: The sender is untrustworthy. So the leader sends an “ERROR” message to the successor to stop the transmission session of the warning. The “ERROR” message contains the Id of the sender.

• State 3: The Data field is falsified by a malicious node. In this case, the leader sends a “CorVALIDATION” to the successor containing the original warning message received by the vehicle which triggered first the alarm. The structure of the “CorVALIDATION” message is similar to the "VALIDATION" message structure but it contains also the field Data describing the triggered alert.

At the end of each statement, the group leader updates the trust values (TV)s and the Cooperation Counters (CC)s of the vehicles which participated in the warning transmission session according to their behaviors.

This verification process is repeated by each successor receiving the “ALARM” message until the end of the transmission session when the last vehicle which received the “ALARM” message has no successor.

3.2.1.3 Task 3: Revocation

The revocation from a group can be a partial revocation or a total revocation. The first form handles the case of vehicles which pass through a group leader for many times. in this case the trust value of the correspondent vehicle saved by the GL will not be deleted. The exit of a vehicle

can be explicit by sending an "EXIT" message to the GL or it can be implicit when the GL doesn't receive message from the vehicle for a period of time. The exit time is saved by the GL into a timestamp to be used in the total revocation that is launched periodically for all the trust model items. For each entry in the trust model, the GL computes the duration between the timestamp saved for the last exit and the current time. If this duration exceeds a threshold, the item should be deleted.

3.2.2 Knowledge base

For registration purposes, we chose to apply a knowledge base system to be used to make appropriate decisions about received alert messages. This system is depicted in figure 3.

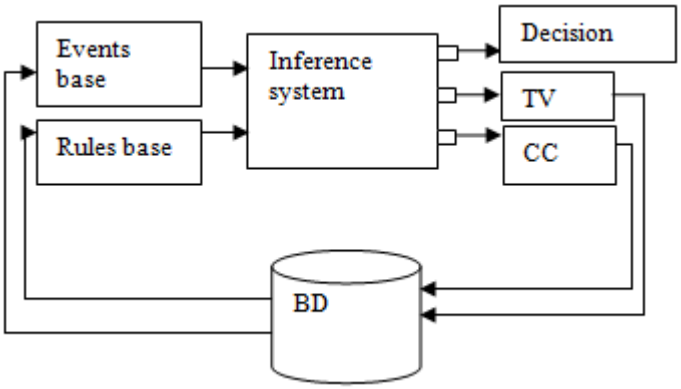

Fig. 3 knowledge base system

3.2.2.1 Events base

Events base contains vehicle properties (idVehicle, position, speed, acceleration …), the trust model structure (idVehicles of neighbors, TVs of neighbors, CCs of neighbors) and all possible road events (Accident (timeA, positionA), Obstacle (timeO, positionO).

3.2.2.2 Rules base

The rules base is a set of rules defining the action list of a vehicle after receiving a message. The vehicle behaviour depends on the message type and the parameters values registered in the Events base. The knowledge base process is the same as a traditional Inference system. It begins by the reception of a new message by a vehicle and it finishes by the generation of the decision about the message if it is accepted or not. Two others parameters are determined: the new trust value (TV) and the new Cooperation Counter of the vehicle source of the message.

3.3 Cooperation model

Our approach is totally autonomous with regard to the external infrastructure. It aims at detecting of malicious vehicles. Our approach guarantees the delivery of the authentic messages while messages containing incorrect information will not be propagated in the vehicular network. The proposed model is a secure and incentive model which has for objective to insure the cooperation encouragement between vehicles by various tools which are:

• The incentive mechanism: if a vehicle A behaves in a cooperative way, the GL modifies the Cooperation Counter "CC" of A by adding points.

• The system of punishment: if a vehicle A behaves in a not cooperative way, the GL modifies the Cooperation Counter "CC" of A by subtracting points.

• The isolation of malicious vehicles: if a vehicle reaches a threshold for the value of "CC", it will be eliminated from the group. So, it will not be covered by the community services.

• The evaluation of the trust level: it is the leading part of our system, the computing of the trust levels of vehicles is necessary to encourage them to cooperate. The GL updates the Trust Value (TV) of Active vehicles according to equation 1:

$$TV = TV + CC \times \propto \quad (1)$$

Where :

- TV is the Trust Value,
- $TV \in [0,1]$
- CC : the value of the vehicle Cooperation Counter
- $CC \in [CC_{max}, CC_{min}]$
- $CC_{min} = -CC_{max}$
- $\propto \in [0, \frac{2}{CC_{max}}]$

3.4 Security model

Currently, because of its huge spread, wireless technology introduces many possible risks to its users. The security module, in our model, provides a solution for these possible risks. Our solution was inspired from the PGP (Pretty Good Privacy) algorithm that is used hugely in a self-organized network as VANET [16]. Social relationships between vehicles are close to those in the PGP system [17]. Unless, the very large amount of source of the complete PGP version makes from its comprehension and use a difficult task [18]. For this reason, we focused only on using the cryptographic and the hash methods used by PGP which are RSA and SHA. Our security module implies the algorithm SHA1-RSA [19]. RSA [20] is a public-key cryptosystem for both encryption and authentication. The public-key cryptography has many advantages [20] as providing the possibility to implement digital signatures. Many existing solutions for VANET security are using RSA [17][21-23]. We applied the SHA-1[24] function with the RSA encryption method. RSA is combined with the SHA1 hashing function to sign a message in this signature suite.

The group leader is in charge of the key distribution in its group. Each vehicle has a pair of public/private key generated by its OBU (On Board Unit). In the announcement step, each vehicle sends its public key to the leader to be used later in the communication step. When a

vehicle A receives an ALARM message from its predecessor B, B sends a CONFIRM message to the leader to verify the trustworthiness of the message and to obtain the public key of A in order to verify the sender authenticity.

4. EVALUATION

We have evaluated our system with respect to two aspects: the number of peers integrated in the community and the average delay in the network.

Table 1 Simulation Parameters

Simulation parameter	Value
Speed Limit of Vehicles	30 Km/s
Acceleration/deceleration	$0.5ms^{-1}/3ms^{-1}$
Number of vehicles	8 to 40
Transmission power	9db, 12db, 15db, 18db, 21db
Simulation time	19s to 80s
Communication protocol	802.11a
Data rate	6Mb/s

.

4.1 Reliability of the suggested protocol

In order to evaluate the efficiency of the suggested model, it's important to start by studying the number of vehicles entering to the community according to a set of parameters such as the Id of the group leader and the transmission power of vehicles. In this section, the simulation time is equal to 60s and the number of vehicles is equal to 26.

4.1.1 Influence of the variation of the group leader identity

First, we have done a set of simulations with the same transmission power (21db). In each one, a different vehicle is designed to be the group leader. Figure 4 shows the percentage of vehicles which are entered in the group for each simulation. The group leader that accepted the great number of vehicles in its group is the vehicle V_0 (88% of the nodes number). The number of members in a group depends on the transmission power of vehicles and the number of vehicles in the leader surrounding.

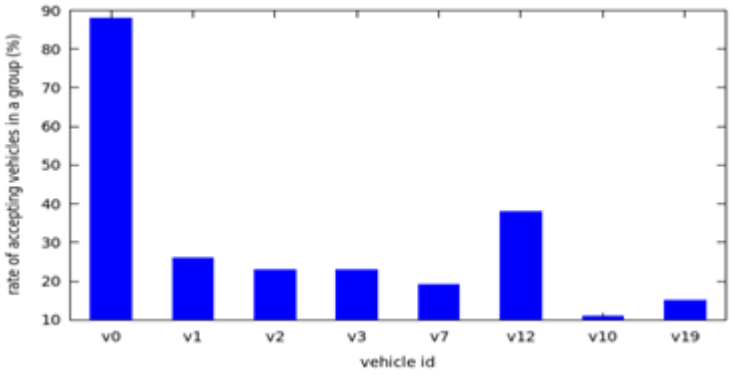

Fig. 4 Accepted vehicles percentage vs. group leader identity

4.1.2 Influence of the variation of the transmission power

In this case, we have launched a new set of simulations for different transmission powers. We have designed the vehicle V_0 as the group leader. As shown in figure 5, for a transmission power equal to 21db relevant to a transmission range of 250-300m, we have found that 88% of the total number of vehicles has undergone the announcement step.

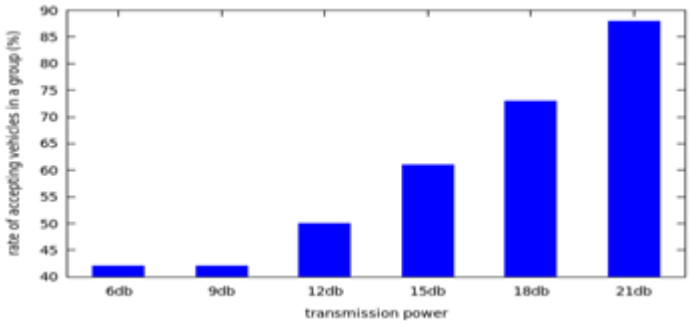

Fig.5 Accepted vehicles percentage vs. transmission power

4.2 Time overhead of SOTM

For evaluation purposes, we simulate our model with a transmission power equal to 21db and with the vehicle V_0 as the group leader. Figure 6 illustrates the end-to-end delay versus the number of nodes for these three speeds. Results obtained by the suggested communication model are compared to the end-to-end delay obtained by the simulation of another approach described in [25]. Authors in [25] proposed an infrastructure based authentication approach for VANET. The simulation results proved that the time overhead introduced by our suggestion is well under the overhead introduced by the approach [25] that ensures only the message authentication and doesn't include an algorithm for a complete trust management as it is the case of our approach. This improvement is due to the self organized approach adapted by our application.

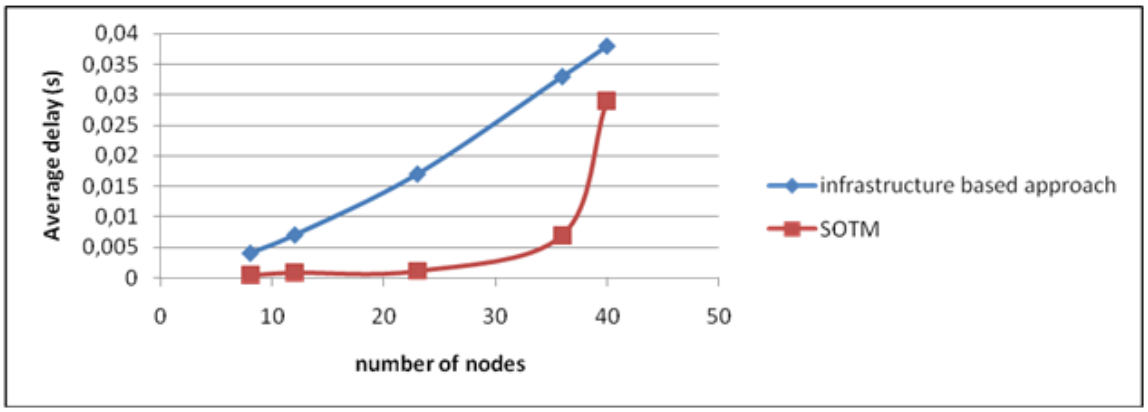

Fig. 6 SOTM vs. an infrastructure based approach

According to figure 6, the overhead introduced by our protocol is under the threshold fixed by the Dedicated Short Range Communications standard (DSRC) [12] that is 100 ms, although, this overhead is caused by messages sent periodically to maintain the linkability between vehicles (ex. the GRE packet). And, it can be reduced by studying and measuring the impact of the periodic time of such a control packet on the network delay in order to obtain the lowest overhead.

5. CONCLUSION

We presented in this paper the SOTM system as a new self organized trust management system for VANET. The SOTM system deals with the registration/updating of vehicles trust values based on historical and runtime vehicles behaviors. Indeed, our model allows the detection and the elimination of misbehaved nodes. And, it interrupts the spread of any false alert message transmitted between vehicles. In addition, simulation results show that the average delay of the proposed system is well under the tolerant delay constraint defined by the DSRC. In order to enhance the SOTM system performance, the privacy issue will be a priority task in the future works.

REFERENCES

[1] G. Samara, W. A. H. Al-Salihy, and R. Sures, “Security issues and challenges of vehicular ad hoc networks (VANET),” in Proceedings of the 4th International Conference on New Trends in Information Science and Service Science (NISS '10), pp. 393–398, Gyeongju-si, Republic of Korea, May 2010

[2] M. M. I. Taha and Y. M. Y. Hasan, “VANET-DSRC protocol for reliable broadcasting of life safety messages,” in Proceedings of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT '07), pp. 104–109, December 2007.

[3] Gillani, S., Khan, I., Qureshi, S., Qayyum, A.: Vehicular ad hoc network (VANET): enabling secure and efficient transportation system. Technical Journal, University of Engineering and Technology, Taxila, vol. 13 (2008)

[4] A. Zouinkhi, A. Ltifi, E. Bajic, E. Rondeau, M. B. Gayed and M. N. Abdelkrim, 'Simulation of active products cooperation for active security management', 8th International Conference of Modeling and Simulation, MOSIM'10, May 10-12, 2010, Hammamet, Tunisia, 2010

[5] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in Proceedings of VANET, 2009, pp. 89–98.

[6] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557– 1568, Oct. 2007.

[7] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in Proceedings of the 67th IEEE Vehicular Technology Conference (VTC Spring), 2008.

[8] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in Proceedings of VANET, 2004.

[9] M. Gerlach, "Trust for vehicular applications," in Proceedings of the International Symposium on Autonomous Decentralized Systems, 2007.

[10] Z. Wang and C. Chigan ,"Cooperation Enhancement for Message Transmission in VANETs", Wireless Personal Communications, Vol. 43, No.1, pp. 141-156, 2007.

[11] J. Hortelano, J.C. Ruiz and P. Manzoni, "Evaluating the Uselfusness of Watchdogs for Intrusion Detection in VANETs", IEEE International Conference on Communications Workshops, ICC Workshops, 2010.

[12] Jagdeep Kaur, Er.Parminder Singh,"Performance Comparison Between Unicast And Multicast Protocols In Vanets", International Journal of Advanced Technology & Engineering Research , Volume 3, Issue 1, Jan. 2013, pp109-115

[13] Adil Mudasir Malla, Ravi Kant Sahu, "A Review on Vehicle to Vehicle Communication Protocols in VANETs", IJARCSSE, Volume 3, Issue 2, February. 2013

[14] R. S. Shukla, I. A. Khan, N. Tyagi, "Performance of Modified Edge Based Greedy Routing Algorithm in VANET Using Real City Scenario",Advances in Mechanical Engineering and its , Applications (AMEA) 168 Vol. 2, No. 3, 2012, ISSN 2167-6380

[15] J. Y. Yu and P. H. J. Chong. "A Survey of Clustering Schemes for Mobile Ad Hoc Networks," IEEE Communications Surveys and Tutorials, Vol. 7. No. 1, 2005, pp. 32–48. doi:10.1109/ COMST.2005. 1423333

[16] Randhawa, Navdeep Kaur. "Design and Implementing PGP Algorithm in Vehicular Adhoc Networks (VANETs)," International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp. 647-650

[17] Shafiullah Khan and Al-Sakib Khan Pathan, "Wireless Networks and Security: Issues, Challenges and Research Trends", Springer Series: Signals and Communication Technology, 2013, pp. 107-132, ISBN 978-3-642-36168-5

[18] Kurniawan, Y., Albone, A., & Rahyuwibowo, H. The design of mini PGP security. International Conference on the Electrical Engineering and Informatics (ICEEI), Indonesia, 17-19 July, 2011.

[19] Sophia A-J. A Score Based Trustworthy Declaration Scheme For Vanets, International Journal of Engineering Research and Applications, 2014; 4(3); 542-544.

[20] Rivest R, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 1978; 21(2): 120–126.

[21] Serna J., Luna J. Medina M. Geolocation-based Trust for Vanet's Privacy. Journal of Information Assurance and Security 2009; 4(5):432-439.

[22] Alangudi B-N, Mahalakshmi R-S. Privacy Preserving Authentication for Security in VANET. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 2014; 2(1): 200-203.

[23] Verma M, Dijiang H. SeGCom: secure group communication in VANETs. In Proceedings of 6th IEEE consumer communications and networking conference (CCNC 2009), Las Vegas, January 2009.

[24] Zhang J-P, Chen C, and Cohen R. Trust based decision making on message relay and local actions in VANET. Journal of Security Communication Networks, 2013; 6(1): 1-14.

[25] Chaurasia B-K, Verma S. Infrastructure based Authentication in VANETs. International Journal of Multimedia and Ubiquitous Engineering 2011; 6(2): 41-54.

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).