Adv Syst Sci Appl 2019; **2**:80–89
http://ijassa.ipu.ru/index.php/ijassa/article/view/707

AODV-based Key Management in VANET

Chaima BENSAID[1*], Sofiane BOUKLI-HACENE [1]

[1]*EEDIS Laboratory , Computer science department, Djillali Liabes University at Sidi bel abbes , Sidi Bel Abbes , Algeria*
E-mail: chaimaa184@hotmail.fr , boukli@gmail.com

Received February 23, 2019; Revised June 21, 2019; Published July 10, 2019

Abstract: Vehicular ad hoc network (VANET) is a self-organized multi hop system comprised by multiple vehicles. This kind of network offers different kind of communication such as Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. The V2V communication a folk of Mobile ad hoc network(Manet). It is characterized by a high mobility, dynamic topology, lack of centralized control infrastructure and a non secured shared media. Similar to Manet, V2V is vulnerable to a many types of attacks such as blackhole, sybil and Denial of service attack. Security in such cases is primordial. Many studies have addressed this issue and many solutions have been proposed. One of the most promising studies used Distribution Certification authority (DCA) to secure communication within VANETs networks. In this paper, we propose a new method of certification based on the study of the behavior of each node based on AODV routing protocol. The operational performance is evaluated with rigorous analysis and extensive simulation study. Our approach reduces certificate with 6.01 to 69.42% less certificates.

Keywords: VANET,AODV, clustering , trust based mechanism.

1. INTRODUCTION

VANET is a network in which a mobile node is a smart vehicle equipped with a sensors. It offers three types of communication: Vehicles to Vehicles (V2V) and vehicles to road side unit infrastructure (V2I) and hybrid communication. Many researches state that V2V VANET communication are vulnerable to a lot of attacks because the dynamic topology and the use of wireless links. To secure these communications a security mechanism is essential.

A Public Key Infrastructure assists that the users obtain the necessary public keys, these public keys are used to perform cryptographic operations. The CA (Certificate authority) issues the digital certificates and provides the means operations to verify the validity of the certificates. However, this solution is costly and not suitable for the different requirements of the VANETs. Lightweight solutions have been also proposed such as DCA and Mobile Certificate Authority (MOCA). Cluster based CA have been proposed for cluster based routing protocols (Cluster based Routing protocol). These solution suffer from Cluster head (CH) overload because these nodes issue new certificates when a mobile cluster number moves between clusters.

In our paper, we propose a new approach to adopt the PKI in VANET based on the well known routing protocol AODV with a trusted system when an extension is used to predict node migration to adjacent clusters. The trusted system proposed is lightwight and it is based only on neighboring node behavior and the prediction process predict the destination cluster

*Corresponding author: chaimaa184@hotmail.fr

and anticipate certificate issuing which minimize the number of issued certificate and allow certification renewal with in all clusters. Our improvement gives a satisfactory result, where the number of issued certificates has declined by about 69%.

2. AODV ROUTING PROTOCOL

The AODV protocol is a reactive routing protocol [1, 2]. It operates using three types of messages: Request messages (RREQ) and Route REPly messages (RREP) and Route ERRor messages (RERR).

When a node wants to send a data packet to a destination node, it looks in its routing table if a fresh route exists to the destination node. If there exist already a valid path it is use to route packets, else, it launches a Route discovery process by broadcasting a RREQ. Each intermediate nodes check if it is the destination node or it has a fresh route to the destination node. If so, it sends a RREP to the source node. Upon receiving the RREP, the source node uses the discovered route to exchange packets with the destination [3]. These route are not secured, for that many studies have focused on security in VANET. In the next section, we're going to discuss security mechanism in VANET.

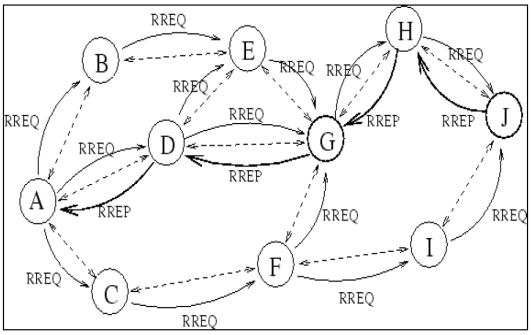

Fig. 2.1. RREQ and RREP packets in AODV

3. KEY DISTRIBUTION

In this section, we present key distribution mechanism present in literature.

Zhou and Hass [4] proposed a partially distributed CA where the key management service (k, n) consists of n servers. Each node has a public/private key, the private key is divided into n shares, one share for each server,and the public key is known to all nodes in the network. Each CA generates a portion of the certificate using its private key and sends it to the combiner. With k correct partial signatures the combiner can construct the complete certificate for member node. It is always possible for a combining node to be compromised by an adversary or be unavailable . Authors have not paid too much attention to the certificate revocation; they proposed a simple approach which is a certification revocation list (CRL).

Yi and Kravet [5] proposed a Distributed Certificate Authority based on threshold cryptography where the signature scheme does not require a combiner C. The Distribution Certification Authority is called Mobile Certificate Authority (MOCA). All nodes are equipped with MP (MOCA certification Protocol), The combination of different parts of the signatures is done by each node. This approach is unsuited for VANET because all certificates must be known by the DCA servers certificates must be known by the DCA servers before providing any access to certification .

A fully distributed certification service based on clustering have proposed by Kong and al [6] . The establishment of certificates in the network is provided by the nodes themselves,

which will be stored by a particular node called CMN (Certificate Management Node) for each cluster. All nodes must request the CMN of the same cluster to collect the certificate strings for each authentication. This system converges to the centralized models where the certificates are stored by a set of special nodes, which puts into question the availability of the certification service especially when CMN became unreachable.

In [7], a based cluster Certification authority architecture is proposed. Each cluster-head (CH) has a CA information table, which contains a list of CA nodes. When a member node requires a certificate, it sends a request to its cluster-head CH to get information about the CA servers. The CH collects information, and forwards to the member node. In this time the node sends the certification request to them. This approach generates lower certificate maintenance overhead by resolving certificate transaction problems. Chaining is done only with trusted nodes that are Cluster head and gateways.

Mukherjee et al in [8] proposed an extention of AODV protocol by adding a new trust mechanism and considering the Successful Cooperation Frequency and Average Encounter Rate as factors to compute for direct trust. modified Dempster-Shafer theory is used to build the recommended trust based on multiple pieces of trust evidence. The trust model is composed of two phases : Route Discovery and Trusted Route Selection which selects the most reliable next hop for routing discard nodes with high mobility and high drop packets.

Ahmed et al. [9] proposed A modified route discovery algorithm to efficiently and securely route data to its destination. This Flooding algorithm is used to define the link failure probability of misbehaving nodes and normal nodes and an Enhanced Multi-Swarm Optimization is used to optimize the discovered route.

4. PROPOSED APPROACH

We propose a cluster based trust model (CBTM) to secure data exchanges in VANETs networks. To degrade network efficiency in a Vanet network, a malicious node sends a great number of RREP to intercept the data packets of its neighbors or to overload the network. for that it uses a very high sequence number in the RREP packet to attract the data packets of its neighbors to go through him to edit or delete them later. In our model, each node in the network is equipped by a cache memory, in which it saves the number of data packets, route request packets (RREQ) and the number of route reply packets (RREPs) received from this node and the sequence number.

Each node will update its cache memory with the following functions :

- recv RREQ () Cache [0] [@src] ++;
- recv Data () Cache [1] [@src] ++;
- recv Reply () Cache [2] [@src] ++;

N_D: the number of data packets received from a node;
N_REQUEST: the number of RREQ packets received from a node;
N_REPLY: the number of RREP packets received from a node;
if $N\_D + N\_REQUEST == 0$ *and* $N\_seq\_dest >>>>> N\_seq\_src$ **then**
  trusted_value=0;
else
  trusted_value=1;
end
if $N\_D + N\_REQUEST! = 0$ *and* $N\_RPLY < N\_D + N\_REQUEST$ **then**
  trusted_value=1;
end
if $N\_D + N\_REQUEST == 0$ *and* $N\_REPLY! = 0$ **then**
  trusted_value=0;
end

Algorithm 1: Computing Trust Value

If the received packet is a RREP, it looks in its cache memory to check the stored values. It will use the following algorithm to decide whether the node is a trusted node or not.

4.1. Clustering

To divide the networks into clusters each node uses its neighbors table. In our implementation, the size of each cluster is empirically fixed to 5, and within each cluster there is a single CH which is the node that has the highest trust value and the higher sequence number in the cluster. In addition, only a trust node can be a cluster member.

4.2. Certification

Hahn and al [10] proposed a model for MANET, where the Cluster-head acts as a CA. The certificate chain allows the exchange of session keys and the encryption / decryption of data. However, any node can be selected as a CA. Due to mobility which is a important feature of the V2V communication, a member node request a new certificate each time it passes from one cluster to another which will overload the number the certificate generating.

Our approach is a trust model based on the study of the total behavior of the member node and if the member node passes of cluster to another, the certificate is broadcast by the gateways.

In this paper, we develop this proposal with detailed simulations study by the well known network simulator NS2.35 [11]. When a node enters in the preemptive region, three signal values are collected and we used the Lagrange interpolation to predict node mobility. The formula of the interpolation is:

$$y = \sum_{i=0}^{n} \left[\frac{\prod_{j=0, j\neq i}^{n} (x - x_j)}{\prod_{j=0, j\neq i}^{n} (x_i - x_j)} \times y_i \right] \tag{4.1}$$

We store three signals values of received data packets and their corresponding receiving time. When two consecutive measurements give the same signal, we store the time of the second occurrence. The expected signal strength P of the packets received from the CH node is computed as follows [12, 13]:

$$P = \left(\frac{(t - t_1) \times (t - t_2)}{(t_0 - t_1) \times (t_0 - t_2)} \times P_0 \right) + \left(\frac{(t - t_0) \times (t - t_2)}{(t_1 - t_0) \times (t_1 - t_2)} \times P_1 \right) + \left(\frac{(t - t_0) \times (t - t_1)}{(t_2 - t_0) \times (t_2 - t_1)} \times P_2 \right) \tag{4.2}$$

Where P_0 , P_1 , P_2 are the measured power strengths at the times t_0 , t_1 , and t_2 respectively. The time t is the sum of time required to send the certificate to Cluster adjacent

$(Inonde\_Period)$ and the difference between t_2 and the average value of the measurement; this value has been determined empirically [14].

$$t = 2 \times t_2 - \left(\frac{t_0 + t_1 + t_2}{3}\right) + Inonde\_Period \tag{4.3}$$

When P is less than the minimum acceptable power $(81dBm)$ a warning message is sent to the CH. The CH sends the certificate to adjacent cluster [12]. When the join the adjacent cluster, the cluster-head compares the nodes address with the received one and saves its certificate.

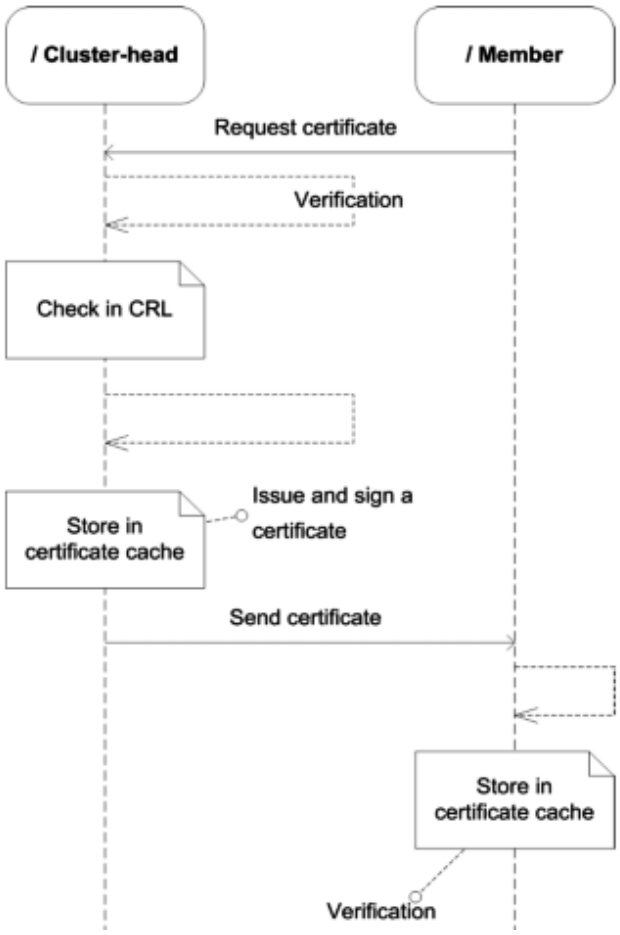

Fig. 4.2. Certficate generation

5. PERFORMANCE EVALUATION

To evaluate the performance we used NS2 simulator . In our approach we used two mobility scenarios, the first is of the city of Malaga and the second is generated by the simulator VANETmobisim .

5.1. Malaga city scenarios

Fig.5.3 present a geographic card of urban VANET scenarios from the downtown of Malaga, Spain [15, 16] . It is composed of three areas U1 , U2 and U3. Detailed parameters of the simulation area is presented in the table 5.1.

Table 5.1. VANET scenarios details

Scenario	Area size	Number of vehicules	Number of connections
U1	$120000m^2$	60	10
			15
U2	$240000m^2$	60	20
U3	$360000m^2$	60	30
			40

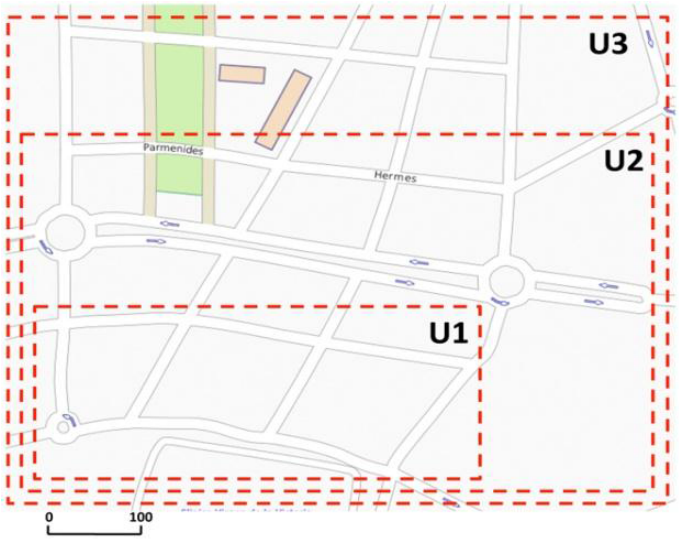

Fig. 5.3. Malaga urban areas

In this scenario 60 vehicles are simulated. Each of them use AODV routing protocol. A CBR application over UDP is used to simulate data transmission between pairs of communicating nodes where packet of 1 KB are sent using a rate of 100 kpbs during 180s. Table 5.2 summarize all used parameters.

Table 5.2. simulation paramaters

Parameters	Value
Propagation Model	Nakagami
PHY layer	IEEE 802.11p
MAC layer	IEEE 802.11p
Routing layer	AODV
Transport layer	UDP
CBR packet size	1024 bytes
CBR packet rate	100kbps
Simulation time	180 s

5.2. VANETmobisim scenarios

The Vehicular Ad Hoc Networks Mobility Simulator (VANETMobiSim) [17] is a set of extensions to user mobility modeling framework CanuMobiSim, used by the CANU (Communication in AdHoc Networks for Ubiquitous Computing) Research Group, University of Stuttgart. It includes a visualization module, mobility models, as well as various formats parsers for geographic data sources. This framework is easily extendable and it is based on the concept of pluggable modules. The set of extensions provided by VANETMobiSim consists mainly on a vehicular spatial model using GDF-compliant data structures, and a set of vehicular-oriented mobility models.

Table 5.3 details all parameters used in this scenario where protocol is under attack.

Table 5.3. simulation paramaters

Parameters	Value
Propagation Model	Nakagami
PHY layer	IEEE 802.11p
MAC layer	IEEE 802.11p
Area size	1000*1000 m
Vehicule speed	from 8.33 to 13.89 m/s
CBR packet size	1024 bytes
CBR packet rate	100kbps
Simulation time	900 s
Number of malicious nodes	3

The well-known metrics to evaluate routing protocol is used in our study :

- Packet Delivery Ratio (PDR): represents the percentage of packets delivered to their destinations .
- The average latency of data packets (Delay): This is the average time required to deliver data packets from the source to the destination successfully.
- Additive costs (overhead): This criterion illustrates the amount of additives cost required for each received data packet.
- Dropped packet: Number of dropped packets due to either link failure or by the malicious node.
- Certificate overhead: the number of certificates sent in network.

Simulation scenarios are :

- AODV vanetmobisim denotes AODV under attack.
- CBTM vanetmobisim represent our approach under attack used vatenmobisim scenario.
- AODV Malaga denotes AODV under attack.
- CBTM malaga represent our approach under attack used Malaga scenario.

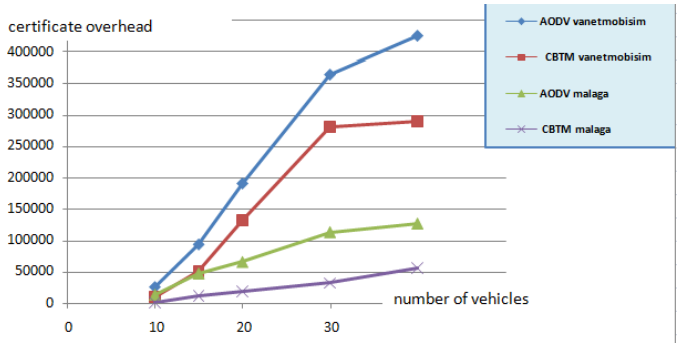

Fig. 5.4. certificate overhead

Fig.5.4 shows the certificate overhead. We observe that the overhead increase high because many nodes request a new certificate from CA and from adjacent CA when a node moves. However, we depict that, our approach outperforms the original with 6.01% to 44.88% less certificates by malaga mobility model and 40.40% to 69.42% less certificates by the model generated by VANETmobisim.

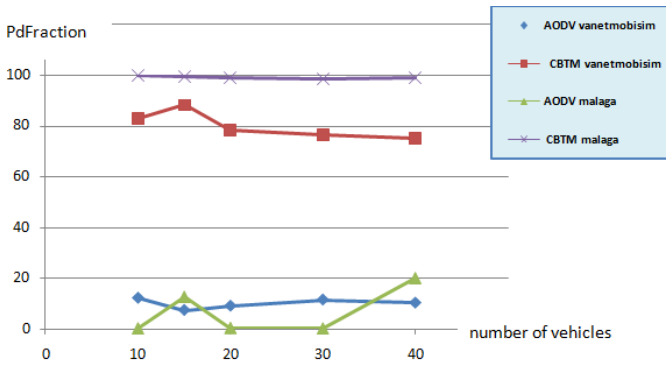

Fig. 5.5. Packet Delivery Fraction

The Fig. 5.5 shows the decreasing evolution of PDF in protocol AODV under attack against to our approach with two mobility models. When the number of vehicles is high, the PDF of our approach register a small degradation. This is due to frequent network topology changes with a high number of connections. We also observe that if the number of vehicles increases the PDF increases for our solution. In the AODV protocol under attack the PDF reach 19.98% .

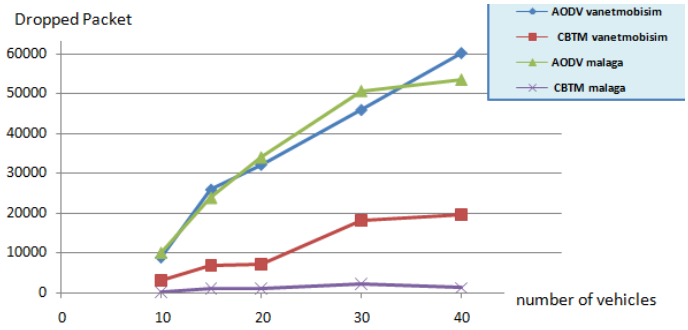

Fig. 5.6. Dropped packet

The Fig. 5.6 presents the number of dropped packets depending on the number of vehicles. In our proposal, with 10 sources of connection, the number of lost packets is 69 and almost no significant against to the AODV under attack 9971 packets in malaga mobility model. Whereas the number of connections increases, it means that there is a lot of data packet sent. In this case, the malicious node intercepts a large quantity of packet so the rate of dropped packet, but in our proposal is a little minimal.

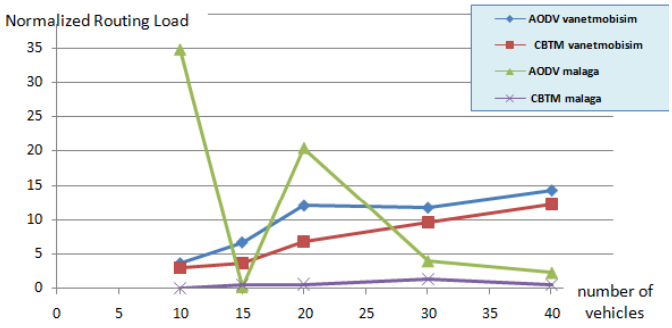

Fig. 5.7. Normalized routing load

The simulation results in Fig. 5.7 show that our proposal is a small routing head relative to AODV under attack. This is due to the fact that when the packet is not received in the right destination, the source node attempts to repair the paths with RRER packets.

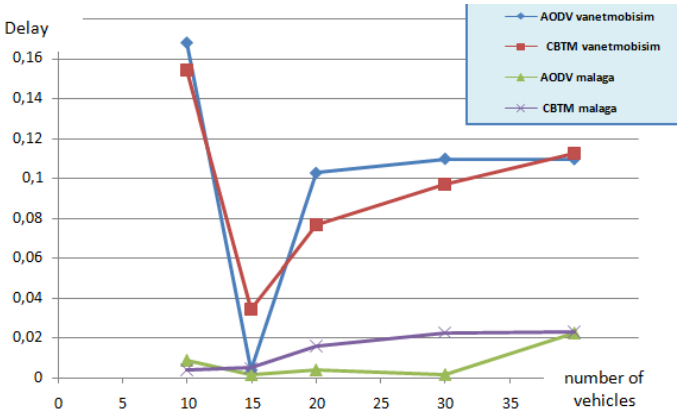

Fig. 5.8. Communication Delay

The Fig. 5.8 shows the evolution of the average end to end delay, depending on number of vehicles in our approach and the AODV under attacks with two mobility models. It is found that the time required by our Proposal is higher than the AODV under attack. This can be justified by using an extra process in our solution to create the certificates and update him.

6. CONCLUSION

In this paper, we presented the different approaches proposed based on PKI in VANET. We also presented a new proposal based on trusted model.

In Our proposal, we interested to V2V communication system where the cluster-head node acts as a virtual CA The main idea is to compute a confidence level for each node by traking its behavior and avoiding the issue of new certificate request in case a node moves.

Our approach reduces certificate with 6.01% to 44.88% less certificates by malaga mobility model and 40.40% to 69.42% less certificates by the model generated by VANETmobisim.

REFERENCES

1. Gupta, P., Goel, P., Varshney, P., & Tyagi, N. (2019). Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET. In Smart Innovations in Communication and Computational Sciences (pp. 271-279). Springer, Singapore.
2. Kandali, K., & Bennis, H. (2018, July). Performance Assessment of AODV, DSR and DSDV in an Urban VANET Scenario. In International Conference on Advanced Intelligent Systems for Sustainable Development (pp. 98-109). Springer, Cham.
3. Perkins, C. E., Belding-Royer, E. M., & Das, S. R. (2002). Mobile Ad Hoc Networking Working Group-Internet Draft.
4. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. IEEE network, 13(6), 24-30.
5. Yi, S., & Kravets, R. (2004). MOCA: Mobile certificate authority for wireless ad hoc networks.
6. Kong, J., Zerfos, P., Luo, H., Lu, S., & Zhang, L. (2001, November). Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks. In icnp (Vol. 1, pp. 251-260).

7. Dong, Y., Sui, A. F., Yiu, S. M., Li, V. O., & Hui, L. C. (2007). Providing distributed certificate authority service in cluster-based mobile ad hoc networks. Computer Communications, 30(11-12), 2442-2452.
8. Mukherjee, S., Chattopadhyay, M., Chattopadhyay, S., & Kar, P. (2018). EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET. In Advanced Computing and Systems for Security (pp. 135-151). Springer, Singapore.
9. Ahmed, M. N., Abdullah, A. H., Chizari, H., & Kaiwartya, O. (2017). F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs. Journal of King Saud University-Computer and Information Sciences, 29(3), 269-280.
10. G. Hahn, T. Kwon, S. Kim, & J. Song, "Cluster-Based Certificate Chain for Mobile Ad Hoc Networks," in International Conference on Computational Science and Applications (ICCSA) , pp. 769-778, 2006.
11. Issariyakul, T., & Hossain, E. (2011). Introduction to network simulator NS2. Berlin: Springer
12. Boukli-Hacene, S. , Lehireche, A., & Meddahi, A. (2006). Predictive preemptive ad hoc on-demand distance vector routing. Malaysian Journal of Computer Science, 19(2), 189-195.
13. Laroui, M., Sellami, A., Nour, B., Moungla, H., Afifi, H., & Boukli Hacene, S. (2018, December). Driving path stability in VANETs. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.
14. Boukli-Hacene, S., Ouali, A., & Bassou, A. (2014). Predictive preemptive certificate transfer in cluster-based certificate chain. International Journal of Communication Networks and Information Security, 6(1), 44.
15. Toutouh, J., & Alba, E. (2011, July). An efficient routing protocol for green communications in vehicular ad-hoc networks. In Proceedings of the 13th annual conference companion on Genetic and evolutionary computation (pp. 719-726). ACM.
16. Malaga city downtown scenario . http://neo.lcc.uma.es/staff/jamal/VANET/?q=node/11
17. VANETmobisim manuel, (2006) Institut Eurcom/Politecnico di Torino

