

RESEARCH ARTICLE

A secure cluster-based architecture for certificates management in vehicular networks

Tahani Gazdar^{1,2}, Abderrahim Benslimane^{2*}, Abdelfettah Belghith¹ and Abderrezak Rachedi³

¹ University of Manouba, Tunisia

² University of Avignon, France

³ University of Paris-Est Marne la Vallée, France

ABSTRACT

In this paper, we propose a distributed and dynamic public key infrastructure for vehicular ad hoc networks. We aim to achieve the fundamental security requirements, particularly the authentication, the confidentiality, and a reliable vehicle-to-vehicle data exchange. To make the certification authority (CA) reachable by all vehicles, we distribute its role among a set of dynamically elected vehicles. The election of dynamic CAs is based on a clustering algorithm where the cluster heads will be CAs in their clusters. The cluster heads are elected following two criteria: security and mobility. Due to the important role of the CA in each cluster and to protect it from DOS attacks, we introduce a VANETs dynamic demilitarized zone for vehicular ad hoc networks. Its role is to handle the certification requests sent to the CA from unknown vehicles, and hence, it avoids compromising it. Additionally, we detail the certificates management in the proposed public key infrastructure, and we propose a mechanism to provide anonymous vehicle-to-vehicle communications using pseudonyms. To study the feasibility of our distributed architecture and particularly the clustering algorithm, we propose a probabilistic model considering the speed of vehicles and taking into account the safety distance between vehicles.

We carried out a set of simulations to evaluate the performance of the proposed clustering algorithm in both urban and highway environments. Hence, we study the effects of the transmission range, the speed of vehicles, and the number of trusted vehicles in the network on the stability and the efficiency of the overall proposed architecture. We also study some delays characterizing the certificates management. Our simulation results show that the security of the proposed architecture closely depends on the number of trusted vehicles in the network, and the stability depends on the mobility of vehicles on the road and on the total number of trusted vehicles. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS

VANETs; security; PKI; trust; mobility; VDDZ; clustering; anonymity

*Correspondence

Abderrahim Benslimane, University of Avignon, France.

E-mail: abderrahim.benslimane@univ-avignon.fr

1. INTRODUCTION

A vehicular network is a radio communication system providing integrated, interoperable, and standardized applications to ensure vehicle to vehicle (V2V) and vehicle to infrastructure communications [1]. Vehicular ad hoc networks (VANETs) provide the basis for a wide set of applications in the transportation environment, including safety vehicles, automated tolling, enhanced navigation, road traffic management, and so on. As a result, these applications require a platform for inter-vehicle communication to achieve a reliable intelligent transportation system that allows broadcasting and collecting different types of information (entertainment and safety).

Several standardization efforts are provided to deploy vehicular networks. In the USA, IEEE has produced a set of standards describing a vehicular network architecture called wireless access in vehicular environment (WAVE)—first, the IEEE 802.11p [2], which describes the new features of physical and message authentication code (MAC) layers to support WAVE communications; second, the IEEE 1609 family of standards [3–6], which describes the higher layers in the WAVE architecture.

However, the deployment of VANETs is facing a serious challenge, which is security [7]. For example, it is essential to ensure that critical information cannot be changed by an attacker. Likewise, the system should be able to establish the responsibility of the drivers, and at the

same time, it must protect as much as possible the privacy of drivers and passengers.

According to the IEEE1609.2 standard, which concerns the security services in vehicular networks, vehicles will be authenticated using certificates managed by a certification authority (CA) within a public key infrastructure (PKI) [4]. However, the PKI cannot be directly used in VANETs, because they are designed for centralized and well connected networks. It is worth mentioning that in VANETs, the network topology changes frequently because of the high mobility of vehicles. Besides, deploying a PKI in VANETs with an architecture designed for centralized networks is facing huge challenges [8]. In fact, the classical architecture of PKI is not scalable, and the CA cannot be accessible to all vehicles due to their high mobility. In addition, having one CA for the whole network may create a single point of failure. Road side units (RSUs) can be considered as CA; however, their density may be insufficient particularly in the first steps of the VANETs deployment. Thus, a vehicle can last a long period outside RSUs transmission range.

Therefore, we propose a distributed and dynamic PKI for VANETs to fulfill the requirements of the security particularly the authentication, the confidentiality, and the reliability of data. First, it is distributed because it is based on distributing the role of the central CA among a set of elected vehicles on the road. The presence of infrastructures on the road is optional. Second, it is dynamic because the election of vehicles depends on the topology changes. Unlike the existing solutions such as [9] and [10], our architecture is tailored to vehicular environments using a relative mobility metric. To elect vehicles that will serve as CAs, two metrics are used: the security and the mobility of the vehicles. The security metric relies on the trust level and the number of trusted neighbors of vehicles. To enhance the security of the elected CA and to protect the CA from denial of services, we use a new approach, which consists in forming a VANET dynamic demilitarized zone (VDDZ) by a set of trusted vehicles located at 1-hop from the CA in each cluster. The role of this set of vehicles is to handle the certification requests from unknown vehicles to the CA, to filter out malicious requests, and to prohibit the communications between malicious vehicles and the CA. Further, we propose an efficient mechanism to achieve anonymous V2V communications using pseudonyms.

Unlike [11] and [12] where authors only tagged the security of data propagation, by using our distributed PKI, we aim to guarantee reliable inter-vehicle communications for different applications of VANETs (e-safety and e-infotainment). In this paper, we aim to extend our previous work [13] as follows:

- (1) First, we describe the details of our clustering algorithm process. Besides, we propose an analytical model to study inter-vehicle connectivity. We aim to investigate the impact of the number of trusted vehicles on the size of the VDDZ. As we will see later, a vehicle can be CA only if it has at least one trusted

neighbor in its VDDZ. Hence, a strong connectivity between trusted vehicles enables the efficiency of the clustering algorithm and the stability of the architecture.

- (2) Second, compared with [13], in the current paper, we describe the inner processing of the PKI. Particularly, we present the details of the certification process. Furthermore, we describe different reliable and anonymous communication scenarios within the proposed PKI. Indeed, our proposed architecture achieves secure inter-vehicle communications in different VANET applications—in unicast such as e-infotainment applications and broadcast such as the dissemination of warning messages.
- (3) Third, all simulations are conducted with real VANET scenarios. We consider two mobility models: a highway and an urban environment. We use the mobility simulator for VANETs, SUMO [14] where the vehicles implement a real driver behavior, which takes into account the road state—the congestions, the traffic lights, crosses, and so on.

The rest of the paper is organized as follows. In Section 2, we discuss the related work on current security solutions proposed for VANETs. In Section 3, we describe the used network model, the trust model, and the distributed clustering algorithm. In Section 4, we study the connectivity between the trusted vehicles. In Section 5, we present the details of some scenarios of secured data exchange. Section 6 is devoted to the performance evaluation. In Section 7, we discuss the characteristics of our architecture, and we compare it with other existing architectures. Finally, Section 8 concludes the paper and presents our future works.

2. RELATED WORK

2.1. Challenges and requirements in securing VANETs

The security of communications in VANETs has to meet several requirements [8,10,15,16]. Indeed, the vehicles must authenticate each other. However, almost adopted authentication systems require the abandonment of the vehicles anonymity. For example, to prevent spoofing, the permanent identity of each vehicle is revealed, then the private information of drivers is violated. So, the trade off between privacy and safety requires to take into account legal considerations. In [17], Jakobsson *et al.* studied the feasibility of solutions based on symmetric cryptography. They proposed an authentication protocol using the session key to encrypt the data and generate a MAC, which ensures data integrity. Moreover, they seek to establish a balance between the privacy reservation and authentication requirements in vehicular networks. The problem is that the vehicles have to contact a base station to decrypt and check

messages, which is not feasible because of the real time nature of demands and the very high mobility in VANETs. An authentication protocol with privacy reservation is proposed in [18]. It is a probabilistic approach, which is based on pre-deployed symmetric keys in vehicles. To generate the keys, the key server has a set of P keys, and each vehicle in the network randomly selects a set R of m keys from P . The authentication is carried out using TESLA protocol [19]. To renew and generate keys for new vehicles in the network, a threshold cryptography scheme (t, n) is used, where n is the total number of vehicles and t is the minimum number of vehicles that must cooperate to generate the secret information. Besides, security solutions in VANETs must provide the non-repudiation of messages, the sender of a message cannot deny sending a message. The drivers responsible for an event occurring on the network (i.e., accidents) should be accurately identified. Additionally, the security in VANETs requires data consistency. The legitimacy of messages includes consistency with other messages that are similar because the sender can be legitimate although the message contains false information. It is worth mentioning that for many applications in VANETs, the security solutions must focus on preventing attacks rather than detecting and recovering them because of the life-critical nature of the messages.

2.2. PKI in VANETs

The significant number of vehicles registered in different countries and their routes on long distances require a strong and evolutionary architecture for securing communications in VANETs and implies the need of a certain level of centralization. Indeed, vehicles have to authenticate themselves not only to each other but also to infrastructures installed on the side of the road, they are called RSUs.

Hence, PKI is an efficient solution to enable secure inter vehicles communications. In fact, PKI provides certification to ensure the data integrity and confidentiality, a strong authentication, and the non repudiation. It is based on an asymmetric cryptography algorithm and a trusted third part called CA, which is responsible for certifying the public keys of vehicles. In VANETs, a PKI must be able to compensate for the periodic breaks in connectivity. Furthermore, the CA must always be available in the network and reachable by all vehicles.

To fulfill those requirements, several works such as [9,10] proposed decentralizing the CA's functionalities. In [9], the authors proposed a self-organized key management based on cluster. In fact, they proposed a model of keys management where VANETs are divided into a number of clusters based on mobility. The principle is that any user can sign another user's public key. The set of signatures forms the network of trust relationships. Besides, each vehicle generates its public key and the corresponding private key before joining the network. If a vehicle u believes that a public key pk_v belongs to a certain user v , it issues a certificate to vehicle v signed by its private key Prk_u .

The drawback of this self-organized approach is that trust is transitive, and the system becomes more vulnerable to the intrusion of malicious vehicles. Furthermore, because the critical role of the vehicle signer of the certificates, it must have a high level of trust. That is why, in our architecture, the CA is elected according to its trust level; indeed, only trusted vehicles can be CA.

In [10], Raya *et al.* proposed a distributed scheme for PKI in VANETs consisting in distributing many CAs, each one corresponds to a region. Car manufacturers are also candidate to take the role of CA. In both cases, the different CAs will have to be cross-certified so that vehicles from different regions or different manufacturers can authenticate each other. This will require each vehicle to store the public keys of all CAs for which it needs to check certificates. The shortfall of this proposal is the unavailability of the CA in the case of network disconnection, which is an important challenge to cope with when establishing a PKI for VANETs. This problem is tackled in our proposal by dynamically electing vehicles on the road to serve as CAs that change according to the topology.

In [12], Blum and Eskandarian use a PKI with virtual infrastructure where a set of elected cluster heads (CHs) are responsible for reliably disseminating messages after digitally signing them. This solution is intended only for one type of attack called "intelligent collisions". However, a PKI in VANETs must cope with different types of attacks. Yet, in our proposal, we target different types of VANET applications: e-safety and e-infotainment. In [20], authors proposed a centralized service to manage public keys for VANETs without certification. They aim to improve the scalability compared with certificates based systems.

In [21], Coronado *et al.* proposed an analytical model to study secure service provisioning. The aim is to assign a secure service session parameters to a vehicle that requests a service in district domains. In this work, the inter-domain communication is established through RSUs and session managers. In [22], authors proposed a key distribution protocol based on PKI, they aim to reduce the cost of key distribution. To this end, they established a distributed architecture based on RSUs. A vehicle dynamically requests a key from encountered RSUs to avoid storing a high set of keys. This proposal requires that RSUs must be deployed frequently on the road to make vehicles continually connected to the CA. Another limitation of this approach is that the CA must track vehicles to know their exact positions so it decides to which RSU it must send the keys of vehicles.

Our paper focuses on a dynamic and distributed PKI different from the classical distributed PKI. In fact, in our proposed PKI, the CAs will be dynamically elected according to its relative mobility with respect to its neighbors. Besides, the role of the registration authority (RA) will be ensured by a set of RA vehicles forming the VDDZ. The VDDZ has a direct link with the resistance degree because it is responsible for the protection of the CA vehicles against different attacks.

2.3. Clustering

Many researches are carried out to design new clustering algorithms tailored to vehicular networks. In [23], authors proposed a clustering method where vehicles are arranged in groups. Each group has a header and a tailer located at the front and the rear. The remaining vehicles in the cluster are described as intermediate vehicles. The vehicle at the head or tail of the cluster will elect itself as the header or tailer. This disposal of clusters on the platoon seems to be very efficient for information propagation. However, because the authors do not detail the election process, a complex mechanism to elect the header and the tailer must be used to avoid collisions where several vehicles announce themselves headers or tailers of the same group at the same time.

In [24], authors proposed a location-based approach to form clusters in VANETs. In fact, the roads are dissected into small areas or cells that define a cluster. A vehicle will automatically know which group it belongs to by comparing its GPS position with a preloaded dissection of the area map into cells. The CH, which is the closest vehicle to the center of the cell is dynamically selected. Cells, and hence clusters, overlap in such a way that any vehicle moving from one cell to another remains in the transmission range of both CHs. The same idea is used in [25]. Indeed, the geographical area is dissected in a series of logical grids. Furthermore, the authors consider RSU in the clustering, more precisely, if there is an RSU in the grid, it will be the CH in that grid. Otherwise, a CH election occurs in the vicinity of the grid's center. This approach is efficient because a vehicle will automatically know which group it belongs to. Hence, the group formation will not require any additional communication overhead or delay. However, the high speed of vehicles on roads reduces the stability of the system, and there will be an enormous number of CH changes.

Furthermore, in [26], vehicles are restricted to be in a group if all group members can hear each other. Authors assume that, because vehicles in a group will move relatively to each other and they have the same average velocity, a group can be represented by a single vehicle referred to as the group leader.

In [27], Fan *et al.* focus on the augmentation of two well-known clustering algorithms: lowest-ID [28] and highest degree [29] with two additional traffic information, the position and the average speed of vehicles. In their paper, Fan *et al.* design a utility-based methodology based on the speed and the position of vehicles. In fact, each vehicle periodically broadcasts general network information such as the identity, the position, and the velocity. Upon the receipt of this information, each vehicle chooses a CH by evaluating the utility of each potential head. The vehicle with the highest utility is selected as CH. However, the two algorithms cannot be directly applied to VANETs because they are not designed for high mobility environments. In fact, vehicles enter and leave the network quickly. Thus, CHs may change frequently their

relative position, then the stability of clusters changes unpredictably.

In [30], Wang *et al.* proposed a cluster structure determined by the geographic position of vehicles and the priorities associated with the vehicle traffic information. The algorithm is based on the exchange of periodic messages containing information about vehicles and their corresponding clusters (its identity, its speed, its CH identity, the next vehicles in the path to the CH, ...). On the other hand, and to enhance the stability of the elected CHs, a vehicle, which has the longest trip, is assigned the highest priority. The disadvantage in this proposal is that the driver should set its destination and the desired speed to calculate the vehicle travel time, and this is before starting its trip.

In [31], authors proposed a new clustering scheme named robust mobility adaptive clustering to strategically enable and manage highly dynamic VANETs. It employs a vehicle precedence algorithm to adaptively identify the nearby 1-hop neighbors and select the optimal CH based on the relative mobility, the location, and the direction of travel. Furthermore, clustered vehicles can assume the role of CH, cluster member, or operate in dual state. A dual state vehicle is a CH of its own cluster and a cluster member of one or more other clusters. However, the proposed algorithm is evaluated only for highway scenarios and seems to be efficient only in highway environment. In addition, to find a CH, a vehicle should have updated information about all its 1-hop neighbors.

We notice that all the previous works are only based on a location metric. However, considering the behavior of vehicles and their cooperation with each other in the network is important in the election of the CH. In fact, the elected CH must have a high trust level, because it will manage the cluster. In our proposed architecture, a trust metric is affected to each vehicle, and only trusted vehicles, which have the highest trust metric, can be elected CHs.

3. DYNAMIC AND DISTRIBUTED PKI FOR VANETS

The basic idea of the architecture consists in establishing a dynamic and distributed PKI. We elect vehicles that will be CAs according to a clustering algorithm. The election is based on two metrics: the average relative mobility of vehicles and their trust level.

3.1. Network model and preliminaries

In a VANET, a vehicle's On Board Unit (OBU) communicates with other vehicles' OBUs and fixed infrastructure called Road Side Units (RSU) as shown on Figure 1. We assume the existence of multiple central certification authorities called central CAs (CCAs), each one is responsible for a geographical region. The CCA manages all credentials of the vehicles registered with it. In addition, the RSUs are connected to the local servers and to the CCAs by wire line communications. In general, RSUs

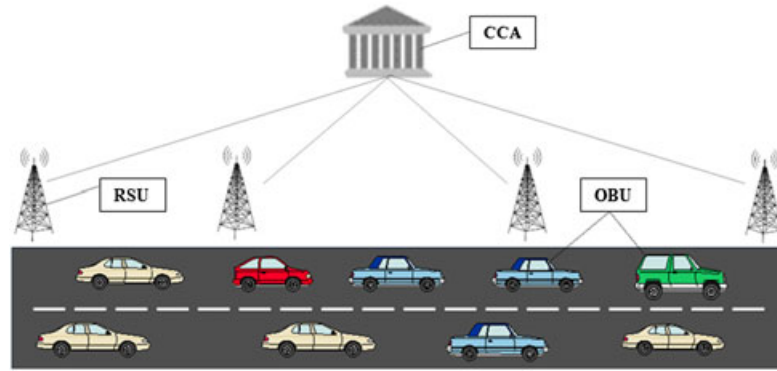


Figure 1. Network model.

have a higher computation capability than vehicles, and we assume that they are trustful and certified by the CCAs of their region. The presence of RSUs is not required for the establishment of our distributed PKI. Nevertheless, they are a part of vehicular networks as described in the IEEE standard of the WAVE architecture [1].

Initially, each vehicle must contact off-line a CCA. He gets a unique identity, a pair of asymmetric keys, and the correspondent long-term certificate; it is signed using the private key of the CCA. Furthermore, we assume that all vehicles are equipped with a tamper proof device responsible for storing cryptographic information and making cryptographic operations.

Our architecture consists in three main modules as presented in Figure 2. First, we use a trust model to assign to each vehicle a trust level reflecting the legitimacy of its behavior. The vehicles, which have the highest trust level are considered trusted, and they can be candidate to serve as CA. Second, to elect vehicles that will be the CAs in their cluster, a clustering algorithm will be executed. It is based on the trust level of vehicles and on their mobility. The third module consists on the inner processing of the proposed PKI, particularly the certification process and the inter-vehicle communications. To study the feasibility and the stability of our architecture, we model the inter-vehicles connectivity using a set of parameters characterizing of the network such as the transmission range,

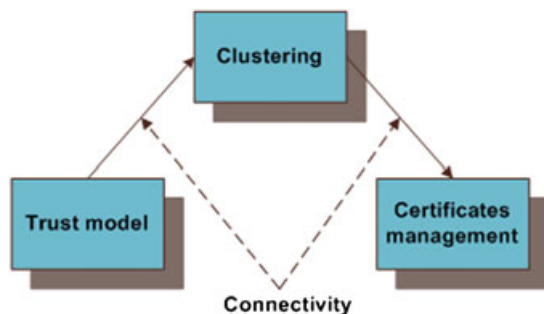


Figure 2. Different modules of the distributed public key infrastructure.

the inter-vehicle distance, the speed, and the number of trusted vehicles.

3.2. Trust model

Our clustering algorithm is based on an important metric, which is the trust level of the vehicles. Because of the important role of the CHs in their clusters, it is worth to consider the behavior of the vehicles represented by the trust metric.

We define a trust metric T_m as a continuous value in the interval $[0-1]$. Each new unknown vehicle starts with $T_m = 0.1$. A vehicle with $T_m = 1$ is defined as trusted (or confident) vehicle.

According to the trust level T_m , we define four roles of vehicles in each cluster:

- (1) CA: Certification authority of a cluster. It certifies the public keys of vehicles belonging to its cluster. A CA has the highest trust level T_m , which is equal to 1.
- (2) RA: Registration authority of a cluster. The main goal of the RA is to protect the CA against attackers to avoid any direct communication between unknown vehicles and the CA. Particularly, they handle and filter the requests of certification toward the CA. The RA must be also trusted with a $T_m = 1$.
- (3) GW: Gateway. It ensures a connection between adjacent clusters. GWs must be certified by at least two different CAs. It has a T_m in $[0.8, 1]$.
- (4) MN: Member node. It represents a member belonging to a cluster. It has an average trust level T_m in $[0.1, 1]$.

Figure 3 shows the state transition diagram where each state represents the vehicle's role in a cluster, and the arrows denote the condition to transit from one state to another according to the trust metric T_m .

We define a VDDZ as the zone located at 1-hop from the CA. It is formed by one or more RA vehicles. The role of the VDDZ is to prevent unknown vehicles from directly

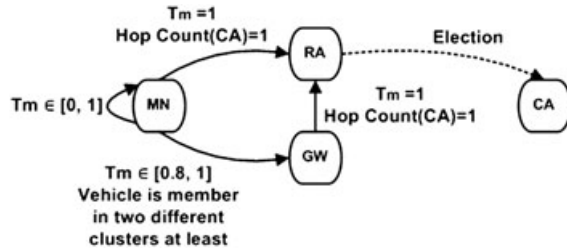


Figure 3. State transition diagram.

communicating with the CA. All guest vehicles must pass by the VDDZ to request a certificate from the CA, and if a vehicle has $T_m = 0$, it is considered malicious, and it will not get certificate.

To increase their T_m , all vehicles having $0 < T_m < 1$ must prove a good behavior and a good cooperation. Indeed, the evaluation of the T_m is based on a hierarchical monitoring process where each vehicle with a high trust level T_m monitors its neighbors with a lower trust level. More precisely, vehicles are invited to broadcast messages about different events occurred on the road, for example, traffic conditions, road conditions, services such as banks, hospitals, restaurants, and so on. When a vehicle A receives such a message from a neighbor B ($T_m(A) \geq T_m(B)$), it evaluates the trustworthiness of the received data, and it records an evaluation report about the behavior of B. In order to compute the average of the trust metric of each vehicle, all vehicles must exchange the calculated trust metrics with their neighbors. Tremendous efficient trust models are proposed in the literature for both MANETs [32] and VANETs [33,34] and [35]. For the time being, the details of updating T_m is out of the scope of the current paper, rather it is the subject of another research work [36].

3.3. Secure and distributed clustering algorithm

A CH, which will become the CA, is selected according to two criteria. First, we consider the security, which relies on the trust metric T_m of a CA candidate, and the number of its trusted neighbors. Second, to guarantee more stability in the cluster, we use the mobility metric, which consists in the relative mobility of a vehicle with respect to all its neighbors.

In our model, only trusted vehicles ($T_m = 1$) can candidate to be CA in their clusters, also each CH is the CA of only one cluster. We further assume that each cluster has a predefined maximum size d equals to the distance in hops count between the CH and the farthest vehicle in its cluster.

Independent of its current state, each vehicle in the network periodically broadcasts a HELLO message at one hop. It contains the identity of the vehicle, its current speed, its current position, its current T_m , and its table of neighbors. Indeed, HELLO messages are useful for vehicles to build and maintain their neighbors' tables. Upon the receipt of a HELLO message, a vehicle calcu-

lates the relative mobility to that vehicle and update its table of neighbors using the information received in the HELLO message.

Only trusted vehicles, which have at least one trusted neighbor located at 1 hop, have the opportunity to candidate to serve as CAs. To declare itself a CA candidate, a vehicle sends an *ELECTION* beacon containing its unique identity, its relative mobility with respect to all its neighbors, and the number of its trusted neighbors. To enhance the security of the elected CA, we take advantage from the human driving habits [11,37]. Everyday, there is a large number of vehicles on the road—people driving to their jobs, means of transport that pass at exact time, and so on. Consequently, RSU can record histories about vehicles patterns and keep trace of vehicles behavior. Thereby, if a trusted vehicle passes all time nearby an RSU and shows a good behavior in terms of legitimacy and trustworthiness of reports that it records about other vehicles, it gets a short-term certificate from RSU that favors it to be CA.

The election beacon message has to be forwarded up to $(d+1)$ hops by vehicles, and on the basis of the information received in beacons, the receivers update their information and decide their status in the cluster. Indeed, the CA candidate having the highest number of trusted vehicles is elected CA. In addition, to enhance the stability of the proposed clustering algorithm, the vehicle having the lowest mobility relatively to its neighbors will be elected CA. On the other hand, if there are candidates certified by RSUs, the CA candidate, which has the newest certificate issued by an RSU, will be elected CA.

During the election process, a vehicle has to acquire different states to join a cluster; they are summarized in Table I.

Upon the entry in the network and for a period q , the vehicle periodically transmits HELLO messages and updates its neighbors' table with the received HELLO messages. If the vehicle receives a HELLO from a CA, it replies with a JOIN message and waits for an accept message from the CA. Otherwise, at the expiration of the timer q , if the vehicle has already received one or more election beacon from CA candidate vehicles, it sorts the set of election beacon according to the relative mobility, the number of trusted neighbors, the issuing time of the certificate from an RSU if there is one, and then the dis-

Table I. States description.

State	Description
INIT_NODE	A starting vehicle.
CA_NODE_CANDIDATE	A vehicle candidate to be a CA.
OR_NODE	An orphan vehicle having no neighbor.
SEARCH_NODE	A vehicle looking for a CA.
WAIT_ACCEPT	A vehicle waiting an ACCEPT message.
WAIT_CA	A vehicle waiting a HELLO message from a CA vehicle.
ACCEPTED_NODE	A vehicle accepted in a cluster.

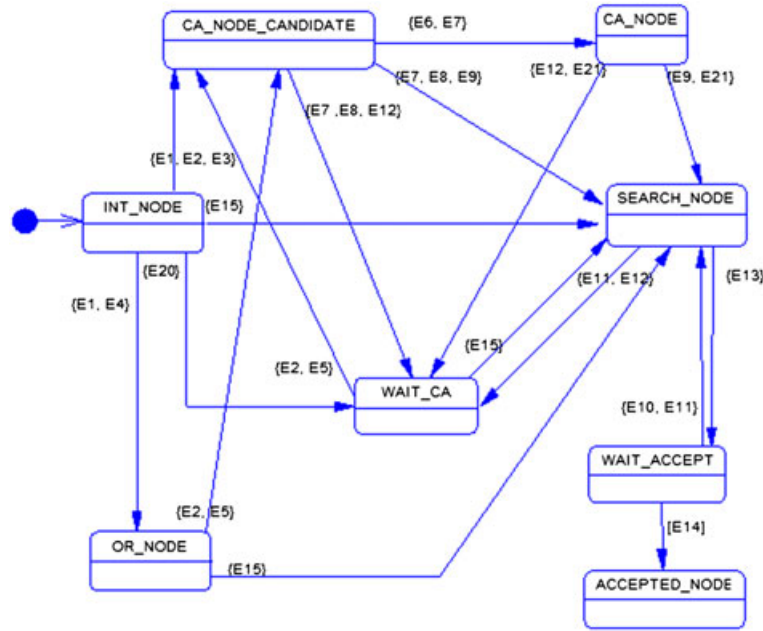


Figure 4. Finite state machine for the clustering algorithm.

Table II. Events description.

Notation	Event description
E1	InitTimer expires
E2	The vehicle is trusted
E3	The vehicle has at least one trusted neighbor
E4	No HELLO is received
E5	A HELLO from a trusted vehicle is received
E6	A Join message is received
E7	ElectTimer expires
E8	No Join message is received
E9	At least a CA candidate exists in neighbors'table
E10	WaitAcceptTimer expires
E11	No Accept message is received OR a Reject message is received
E12	No CA candidate exists in neighbors'table
E13	A Join message is sent
E14	An Accept message is received
E15	A HELLO from a CA vehicle is received
E16	A HelloFromCATimer expires
E17	hop (CA) = 1
E18	hop (CA) > 1
E19	No HELLO from the CA is received
E20	No HELLO from a trusted vehicle is received OR the vehicle is not trusted
E21	No RA vehicle still in the cluster

tance in hop count to the candidate. Hereafter, it sends a JOIN request message to the best candidate according to the previous detailed criteria and waits for an accept notification.

Although, if the vehicle is trusted and does not receive any election beacon and has at least one trusted neighbor,

it can be candidate to serve as CA, so it broadcasts its own election beacon. Then, the CA candidate waits for a certain time, denoted q' , during which it collects JOIN messages from vehicles that elect it as CA. If the CA candidate does not receive any JOIN message, it waits for another election process. Otherwise, it announces itself as CA. A CA vehicle has to transmit periodically a HELLO message, which must be forwarded up to d hops by the cluster members, to maintain the cluster connectivity. In Figure 4, we describe the finite state machine of the proposed algorithm, where states are presented in Table I and events are detailed in Table II.

Upon the acceptance of a new vehicle in a cluster, the CA decides the state of that vehicle among one of the following states: RA, GW, or MN as detailed in Figure 3.

All vehicle members of the clusters have to periodically receive a HELLO message from at least one RA vehicle in the VDDZ of their clusters. Furthermore, all members of the VDDZ must receive HELLO from their CA. If the period expires and no HELLO message is received, then the vehicle is no longer in the cluster, or the cluster does no longer exist.

4. MODELING AND ANALYSIS OF THE CONNECTIVITY IN THE VDDZ

In this section, we study the impact of the density of trusted vehicles on the formation of the clusters.

4.1. Connectivity model

To establish the distributed PKI, the trusted vehicles must collaborate with each other to form the clusters and to

assign the roles of CA and RA in each constructed cluster. Recall that to form a cluster, a candidate for CA must have at least one trusted neighbor. In other words, the existence of at least two trusted vehicles, which are in a direct communication is required. Two vehicles i and j are in direct communication if each one is in the transmission range of the other. We formulate a direct connection between two vehicles i and j by: $(|X_i - X_j| \leq R)$, where X_i (resp. X_j) is the location of vehicle i (resp. j) and R is the transmission range.

In an usual driving scenario, no collision occurs between two succeeding vehicles. Indeed, each driver must respect an inter vehicles distance that makes them safe. We call it the safety distance denoted D_s . We define D_s [38] as follow:

$$D_s > \text{Min}(D_{\max}, \alpha * V(\sigma + V(1/2 * a_r - 1/2 * a_e))) \quad (1)$$

where:

- (1) D_{\max} designates a safety distance, which guarantees that no collision will occur between both vehicles regardless of their velocities,
- (2) α represents a tolerance factor,
- (3) σ is the average reaction time of individual drivers ($0.75s < \sigma < 1.5s$),
- (4) a_r and a_e are the emergency deceleration and regular deceleration respectively,
- (5) V designates the velocity of vehicles. We assume that vehicles are traveling with the same average speed.

Because i and j should respect D_s , then a direct connection between two vehicles will be formulated as follows:

$$D_s \leq |X_i - X_j| \leq R \quad (2)$$

We assume that n vehicles are distributed in the network, with a Poisson arrival rate λ [32,39] and [40]. The probability that any vehicle i can directly communicate with any vehicle j is:

$$p = \text{Pr}(D_s \leq |X_i - X_j| \leq R) \quad (3)$$

As the inter arrival distance of Poisson sequence is exponentially distributed and memoryless, we get the following probability[†]:

$$p = \text{Pr}(|X_i - X_j| \leq R) - \text{Pr}(|X_i - X_j| \leq D_s) \quad (4)$$

with:

$$\text{Pr}(|X_i - X_j| \leq R) = 1 - e^{-\lambda R} \quad (5)$$

and

$$\text{Pr}(|X_i - X_j| \leq D_s) = 1 - e^{-\lambda D_s} \quad (6)$$

[†] Giving F a probability distribution function and a random variable X , so: $F(a \leq X \leq b) = F(b) - F(a)$

We have then from Equations (3), (5), and (6):

$$p = e^{-\lambda D_s} - e^{-\lambda R} \quad (7)$$

The probability to have $(\theta + 1)$ trusted vehicles directly connected is:

$$P_\theta = \prod_{i=1}^{\theta} (e^{-\lambda D_s} - e^{-\lambda R}) = (e^{-\lambda D_s} - e^{-\lambda R})^\theta \quad (8)$$

Let n be the number of vehicles on the network and k the number of the trusted vehicles ($k \leq n$) among n vehicles. We denote the set of trusted vehicles by K . The probability to have two vehicles i and j in direct communication given that they are trusted is as follows:

$$P = p * \text{Pr}(i \in K) * \text{Pr}(j \in K | i \in K) \quad (9)$$

$$P = p * \left(\frac{k}{n} * \frac{k-1}{n-1} \right) \quad (10)$$

In the general case, the probability to get $\theta + 1$ ($\theta < k$) trusted vehicles directly connected knowing that they are trusted vehicles is:

$$P = P_\theta * \left(\frac{k}{n} * \frac{k-1}{n-1} * \dots * \frac{k-\theta}{n-\theta} \right) = P_\theta * \prod_{i=0}^{\theta} \left(\frac{k-i}{n-i} \right) \quad (11)$$

We investigate the probability to form a VDDZ with θ trusted vehicles, in other words, the probability to have $\theta+1$ trusted vehicles in direct communication in the VDDZ, as indicated in Equation (11). We consider $\alpha = 3$, $\sigma = 1.5$, $a_r = 5$, and $a_e = 8$.

4.2. Analytical results

4.2.1. Impact of the transmission range.

To have a first idea about the variation of P according to R and D_s , we plot in Figure 5 probability P that two vehicles are directly connected in the case of 100% of trusted cars. We notice that P increases when the transmission range denoted by R rises. However, the increase of the speed induces the decrease of P . This behavior is due to the fact that the security distance rises when the average speed is getting higher. As a result, the vehicles are increasingly so distant on the road that we obtain much higher value in Equation (6). Moreover, P is much more interesting for a high transmission range R .

We plot in Figures 6 and 7 the probability to get $\theta + 1$ trusted vehicles directly connected in the case of different transmission ranges.

Figure 6 shows the probability to get $\theta + 1$ trusted vehicles directly connected according to the percentage of trusted vehicles in the network in the case of a transmission range equal to 350 m.

We notice that when the percentage of trusted vehicles grows, the probability to form a VDDZ with a size θ

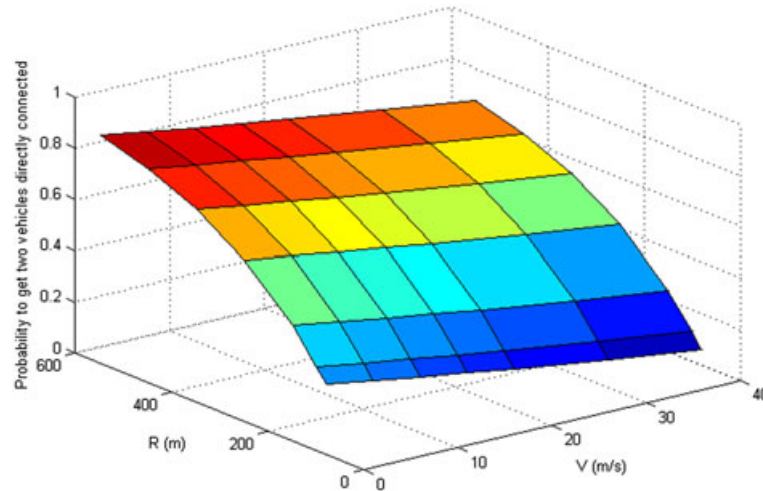


Figure 5. Probability to get two vehicles directly connected.

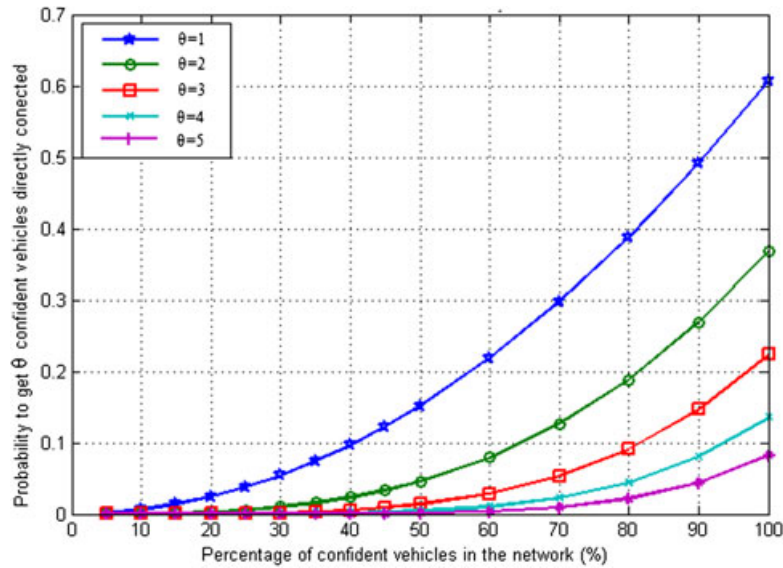


Figure 6. Probability to get a VANETs dynamic demilitarized zone with a degree θ , $R = 350$ m and $V = 25$ m/s.

increases. However, the probability to have a VDDZ with a small size θ ($\theta = 1$, $\theta = 2$) is greater than the probability to have a VDDZ with a high size θ ($\theta = 4$ and $\theta = 5$).

In Figure 7, probability P for a transmission range equal to 550 m increases compared with the case of $R = 350$ m plotted in Figure 6, it reaches 0.8 with $\theta = 1$ (only one vehicle in the VDDZ). This is the minimum and good enough degree to form a VDDZ and hence, to form a cluster. This behavior of curves is due to the fact that the number of neighbors, located at 1-hop from the CA, increases with a large transmission range so that the connectivity of vehicles raises. In all figures, we remark that P is always inferior to 1 and does not reach this value because the vehicles must move with respect of the security distance D_s with their preceding and following neighbors.

So that, $P = 1$ can be reached only if $D_s \rightarrow 0$, which means that vehicles are stationary or in the case of very dense scenarios.

4.2.2. Impact of the speed.

The following figures show probability P according to the percentage of trusted vehicles in the network for a speed of 10 and 30 m/s and a transmission range of 450 m.

As depicted in Figures 8 and 9, P decreases when the speed rises. It reaches 0.8 for 10 m/s and only 0.68 when the average speed is 30 m/s. This is due to the augmentation in the D_s when the speed gets higher. On the other hand, P strongly depends on the percentage of trusted vehicles in the network given that only trusted vehicles located at one hop from their CA can be members of the VDDZ.

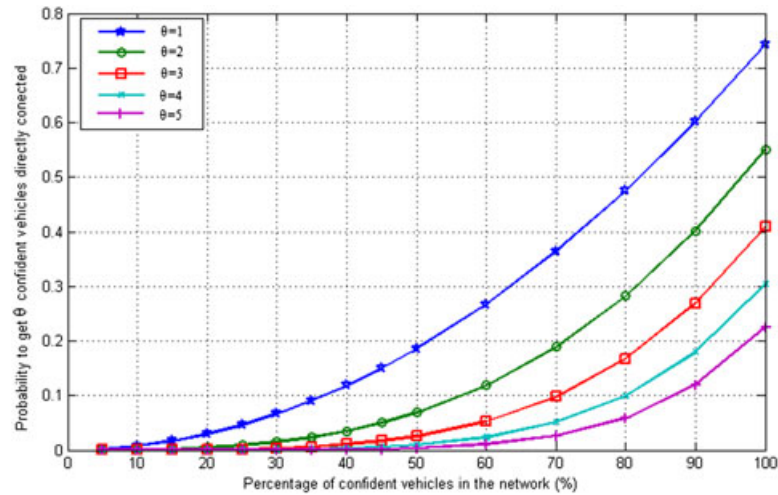


Figure 7. Probability to get a VANETs dynamic demilitarized zone with a degree θ , $R = 550$ m and $V = 25$ m/s.

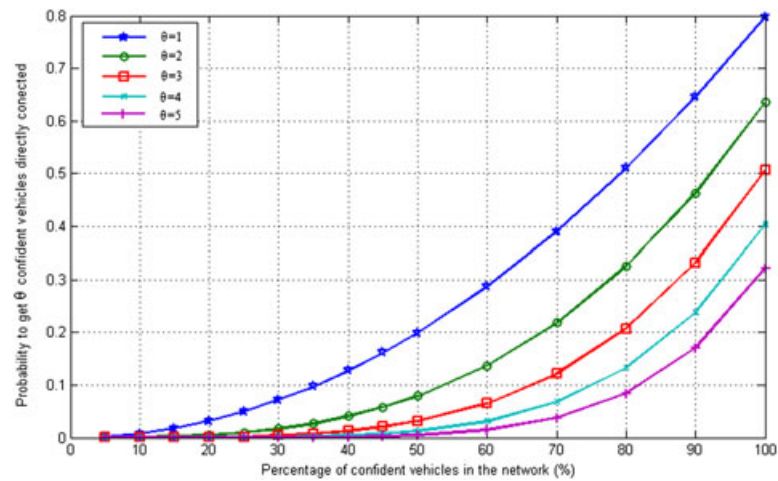


Figure 8. Probability to get a VANETs dynamic demilitarized zone with a degree θ , $R = 450$ m and $V = 10$ m/s.

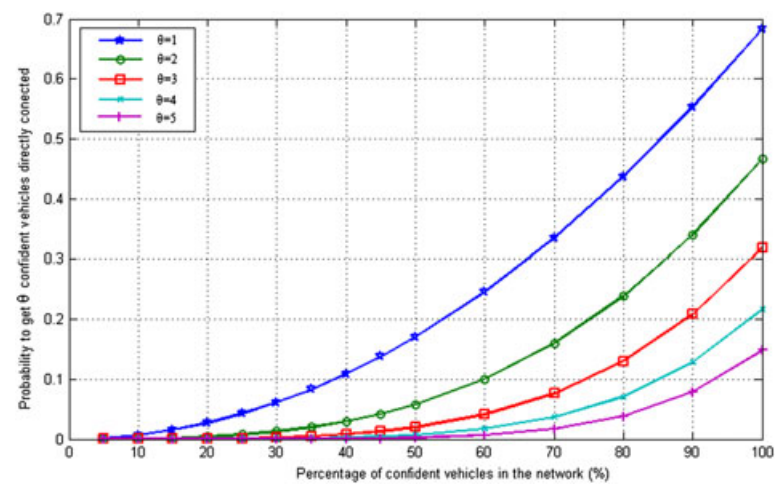


Figure 9. Probability to get a VDDZ with a degree θ , $R = 450$ m and $V = 30$ m/s.

This probability P may be more favorable if we consider a higher value of transmission range R , but we currently restrict our study to $R = 550$ m.

5. CERTIFICATES MANAGEMENT AND SECURING COMMUNICATIONS

The objective of this section is to detail the certification process, the certificates management, and how to ensure a secure and anonymous communications between peers after the establishment of the PKI. Particularly, we consider two types of applications in VANETs: unicast and broadcast.

5.1. Cluster configuration

Upon the formation of a cluster, the CA_i vehicle should first, generate its pseudo identity PID_i and its pseudo pair of keys short term $(PK_{PID_i}^+, PK_{PID_i}^-)$ as it will be detailed in the following section. Next, it generates a certificate associated to the short-term pair of keys signed by its long-term private key. After, the CA (PID_i) establishes a group key (GK_k), which will be used only in the VDDZ for communications between the CA and RAs and between RAs. All members in the VDDZ of cluster k have a common pseudonym $vddz_k$ to which is associated a pair of keys $(K_{vddz_k}^+, K_{vddz_k}^-)$. Thus, in each packet transmitted to the CA_k or one of the RAs, the destination address should be set as $vddz_k$. Hence, we guarantee the anonymity of the CA and RA vehicles, and no vehicle even located at one hop from the CA knows the real identity of the CA or communicates directly with it. Each time an RA leaves the VDDZ, the CA renews the pair of pseudo keys to avoid that it tries to disclose exchanged information after its departure from the cluster.

If a vehicle leaves its cluster, it generates a new pair of keys and asks for a certificate from a new CA. However, at a given time, a vehicle possesses only one valid pair of keys unless it is a GW. All certificates issued by a CA in a cluster have a time to live T , if it expires and the vehicles are still attached to their cluster; they must renew their certificates. In Table III, we present all notations that will be used.

5.2. Certification process

Each vehicle uses a pseudonym and short-term asymmetric pseudo keys. So, to generate pseudonyms and pseudo keys, we consider an additive group $G1$ and a multiplicative group $G2$ with the same prime order q , and a bilinear map $f : G1 * G1 \rightarrow G2$. In addition, two hash functions $H1$ and $H2$ are defined as follows:

$$H1 : \{0, 1\}^* \rightarrow G1 \quad (12)$$

$$H2 : \{0, 1\}^* \rightarrow \{0, 1\}^l \quad (13)$$

Table III. Notations.

ID_i	Identity of vehicle i
PID_i	Pseudo identity of vehicle i
(K_i^+, K_i^-)	Long-term pair of keys of V_i
(PK_i^+, PK_i^-)	Short-term pair of pseudo keys of V_i
$E_{k_i}^-$	Encryption algorithm using k_i^-
$E_{k_i}^+$	Encryption algorithm using k_i^+
C_p^i	Long-term (permanent) certificate of V_i
C_T^i	Short-term (temporary) certificate of V_i
CC_j^i	Cross certificate issued by CA_j to CA_i
GK_k	Group key in the VDDZ of cluster k
$vddz_k$	Identity of the VDDZ in cluster k
$Sig_{k_i}^-$	Signature of vehicle A calculated using private key k_i^- of vehicle i

where l bit is the output length. The pseudo identity and the correspondent pair of keys of vehicle ID_i are generated as follows:

$$PID_i = r_{1i} \cdot H1(ID_i) \quad (14)$$

$$PK_i^+ = r_{2i} \cdot H1(K_i^+) \quad (15)$$

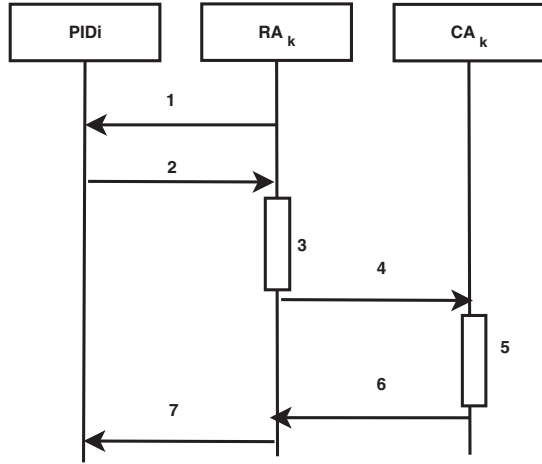
$$PK_i^- = r_{3i} \cdot H1(K_i^-) \quad (16)$$

Where r_{1i} , r_{2i} , r_{3i} are random numbers generated by vehicle ID_i .

After, vehicle ID_i proceeds to get a certificate corresponding to its pair of pseudo keys from a CA. We consider two scenarios: either the vehicle participated in the election of the CA vehicle or it just gets the road. In the first case, it will receive the certificate attached to the accept message (Section 3). However, in the second case, the vehicle requests a certificate from the CA. In fact, as detailed in previous sections, in each cluster RA vehicles form the VDDZ and periodically broadcast HELLO messages. Vehicle PID_i detects cluster k in its neighborhood if it receives a HELLO message from VDDZ $vddz_k$. Thus, if vehicle PID_i wants a certificate from a CA, it sends a request to $vddz_k$ source of the HELLO message. Once an RA in $vddz_k$ receives the request from PID_i , it must authenticate it using certificate long-term C_p^i , which is signed by the private key of the CCA.

If V_i is well authenticated, the RA vehicle transmits the request to the CA. Figure 10 presents the details of this scenario:

- (1) HELLO
- (2) $E_{k_{vddz_k}}^+ (PID_i, C_p^i, PK_{PID_i}^+)$
- (3) Authentication of PID_i
- (4) $E_{GK_k} (PID_i, PK_{PID_i}^+)$
- (5) $E_{GK_k} (E_{k_{PID_i}}^+ (certificate))$
- (6) $E_{k_{PID_i}}^+ (certificate)$
- (7) Authentication of RA_k and generation of the certificate for PID_i

Figure 10. Issuing a certificate for vehicle PID_i .

5.3. Securing inter-vehicle communications

5.3.1. Broadcast applications (e-safety).

This type of applications requires that the vehicles, which broadcast messages, are legitimate and have a high level of trust. To this end, we will restrict the dissemination of such messages to trusted vehicles. Indeed, if vehicle A detects an urgent event on the road and it is trusted, then it broadcasts the message after signing it with its private key, otherwise, it sends the alert message to the nearest trusted vehicle in the same cluster. The trusted vehicle, which receives the message, checks the legitimacy of vehicle A using its short-term certificate, then it broadcasts the message.

5.3.2. Unicast applications (e-infotainment).

Consider two vehicles A and B belong to the same cluster, which will exchange data messages. A encrypts the message with B's short-term public key (and vice versa from B to A). B decrypts the message using its short-term private key. Whenever the CA in a cluster no longer exists, the vehicles continue their communication until the validity of their keys expires. At the same time, A and B must find new clusters.

In both previous scenarios, if the communicating vehicles are from different clusters, then they must accomplish a cross certification.

5.3.3. Cross certification.

The cross certification consists in establishing a trust relationship between two CAs, which do not share a common root. In fact, a first CA issues a certificate called "cross certificate" to another CA. In our case, the CA vehicles generate their own short-term certificates and sign them with their long-term private keys. However, if a vehicle wants to communicate with another one, it must use its short-term pair of keys and the corresponding certificate signed by a CA, which is self-certified. Thus, the cross

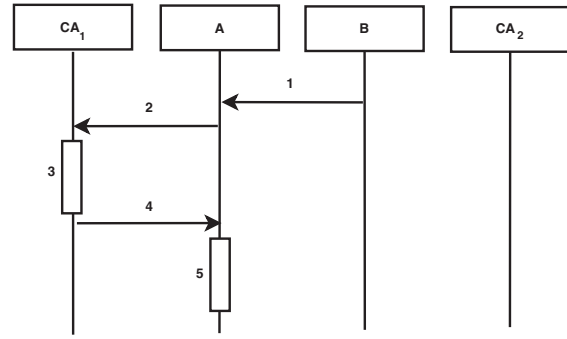


Figure 11. Inter clusters communication.

certification takes place each time two vehicles from different clusters will communicate in broadcast and unicast applications.

Consider two vehicles A and B from different clusters CA_1 and CA_2 , respectively. Then, if A receives a message from vehicle B, it must authenticate it. To this end, A sends C_T^B of B to CA_1 . Then, CA_1 verifies if it is already cross certified with CA_2 . Otherwise, it requests a cross certificate from CA_2 . The cross certification process is well detailed in Figure 11:

- (1) $E_{PK_A^+} \left(M, E_{PK_{CA_2}^+} \right)$
- (2) Request for authentication of B
- (3) Cross certification with CA_2
- (4) 5.Authentication of B

So, to accomplish the cross certificate, CA_1 sends its short-term public key (self-certified) and its long-term certificate C_P^1 . This request will go through the $vddz_1$ and $vddz_2$ to CA_2 . Upon receiving the request for certification, CA_2 must verify that the long-term certificate of CA_1 is well signed by the CCA. In addition, it must verify whether its short-term public key is self-certified. After, it generates the cross certificate and signs it with its short-term private key and retransmits it to CA_1 ; at the same time, CA_2 attaches in the same message a cross certificate request to CA_1 . All communications between a CA and the members of its $vddz_k$ in cluster k are encrypted by group key (GK_k), and any message exchanged between CA_1 and CA_2 is encrypted with their short-term and self-certified public key.

The cross certification process is presented in Figure 12:

- (1) $E_{GK_1} \left(E_{PK_{CA_2}^+} (Request\ for\ cross-certif_1) \right)$
- (2) $E_{K_{vddz_2}^+} \left(E_{PK_{CA_2}^+} (Request\ for\ cross-certif_1) \right)$
- (3) $E_{GK_2} \left(E_{PK_{CA_2}^+} (Request\ for\ cross-certif_1) \right)$
- (4) Authentication of CA_1 and generation of CC_2^1
- (5) $E_{GK_2} \left(E_{PK_{CA_1}^+} (CC_2^1, Request\ for\ cross-certif_2) \right)$

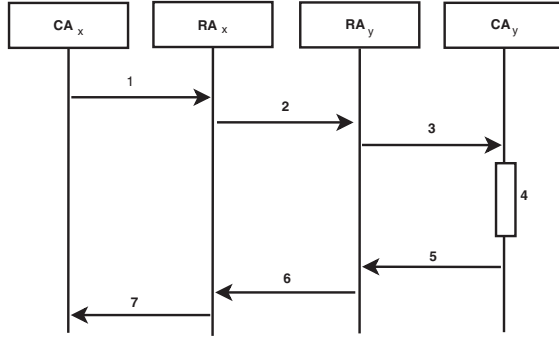


Figure 12. Cross certification process.

- (6) $E_{K_{vdz1}^+} \left(E_{PK_{CA1}^+} \left(CC_2^1, \text{Request for cross-certif}_2 \right) \right)$
- (7) $E_{GK_1} \left(E_{PK_{CA1}^+} \left(CC_2^1, \text{Request for cross-certif}_2 \right) \right)$

Notation:

- (1) Request for cross-certif1 = $\left(PID_{CA1}, Pk_{CA1}^+, C_P^1, Sig_{K_{CA1}^-} \right)$,
- (2) Request for cross-certif2 = $\left(PID_{CA2}, Pk_{CA2}^+, C_P^2, Sig_{K_{CA2}^-} \right)$

6. PERFORMANCE EVALUATION

We conducted a set of simulations to evaluate the proposed architecture and clustering algorithm in the real context vehicular scenarios. Particularly, we investigate the security and the stability of the formation of the cluster while considering different parameters such as the transmission range, the speed, and the density of vehicles.

6.1. Simulation set up

6.1.1. Mobility models.

We use the traffic simulator SUMO [14] to generate our mobility models. It is a microscopic, continuous-space, and discrete-time traffic simulator to model realistic vehicle behavior. SUMO simulates the movement of every single vehicle. In addition, the driver behavior depends on the behavior and the speed of the preceding car. This model exactly implements the real behavior of drivers.

In our simulations, we distinguish two main scenarios: a highway model and an urban model.

Highway scenario We consider a segment of 10 km of highway. It is composed of two lanes, and all vehicles move toward the same direction as shown in Figure 13. All vehicles have a maximum speed of 40 m/s.

Urban scenario We consider a set of four adjacent intersections as shown in Figure 14. Each road is composed of two lanes where vehicles move in the two opposite directions as shown in Figure 14. The distance between each two intersections is of 1000 m. In this scenario, vehicles enter the network from all road end points. The maximum speed of vehicles is 20 m/s. Upon entering the network, each vehicle picks a random destination in the network. In the intersection, the vehicle turns to right or left with a given probability, and each road has a priority Pr.

In both scenarios, trusted vehicles are randomly distributed in the network, and the arrival rate of vehicles is 0.5 vehicles/s. We suppose that the encryption algorithms do not require much time; in simulations, we consider this time equal to 0.

6.1.2. Simulation parameters.

To evaluate the performance of the proposed architecture, we implement the clustering algorithm in the network simulator OMNET++ [41], particularly we used the framework inetmanet. We use the simulation parameters mentioned in Table IV.

All clusters have a predefined size d equal to 3 hops, and the maximum number of members per cluster is 300 nodes. The HELLO period is fixed to 2 s [42,43]. A smaller value might generate a high overhead. However, a value >2 s might delay the update period of the neighbors' tables. Hence, the maintenance of the architecture will not be efficient.

We focused on two main metrics, the stability and the efficiency of the clustering algorithm.

On one hand, the stability is evaluated by the average life time of the CA vehicles. In fact, we measure the average time during which the CA maintains its state. On the other hand, we are interested in the efficiency in terms of the percentage of vehicles attached to clusters. In addition, we will evaluate the average delay required for a new vehicle entering the network, to be attached to a cluster.

6.2. Simulation results

6.2.1. The efficiency of the clustering.

Before investigating the efficiency of the clustering, we need to have an idea about the number of clusters in the

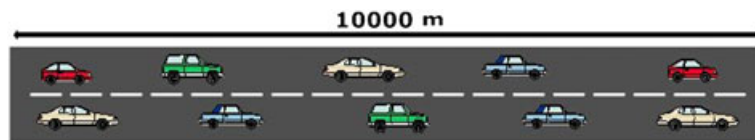


Figure 13. Highway scenario.

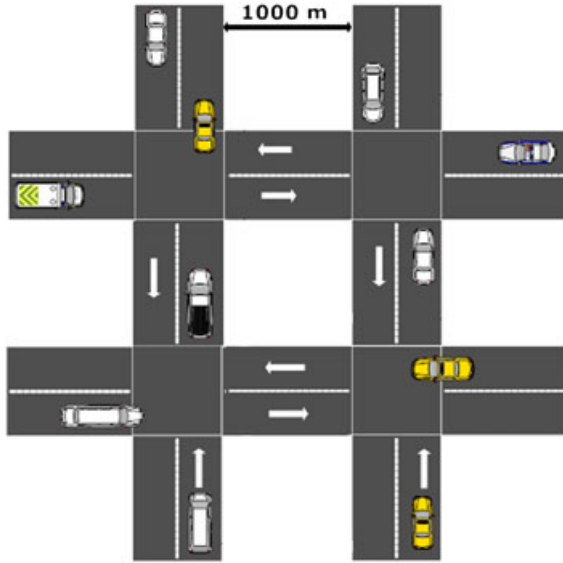


Figure 14. Urban scenario.

Table IV. Simulation parameters.

Parameters	Values in the simulation
Simulation period	500 s
MAC protocol	CSMA/CA
Average speed	[10–40 m/s]
Transmission range	350 m, 550 m
d	3 hops
Maximum vehicles number per cluster	300
HELLO period	2 s

network as well as the number of RAs in each VDDZ because they represent the fundamental role to establish the architecture.

First, we are interested in the number of CAs. We plot in Figure 15 the average number of clusters as a function of the transmission range for each scenario.

We notice that the average number of CA decreases from around 12 to 4 when the transmission range is getting higher in the highway environment. In the urban scenario, it decreases from 14 to 5. In fact, as mentioned previously, all clusters have an equal predefined size d , which is the hop count between the CA and the farthest member in its cluster and an equal maximum number of members in each cluster. Then, the election will be triggered in only two cases. First, all clusters are saturated, and there is no one which can accept new vehicles. Second, a vehicle looking for a cluster cannot reach any CA because the distance that separates it from the CA is too large. The number of CA vehicles depends on the distribution of vehicles on the road (such as congestion, gap, etc.), which is related to the average speed of vehicles and the behavior of drivers. This case may be more encountered in the urban model than in the highway model. That is why in the curve, which

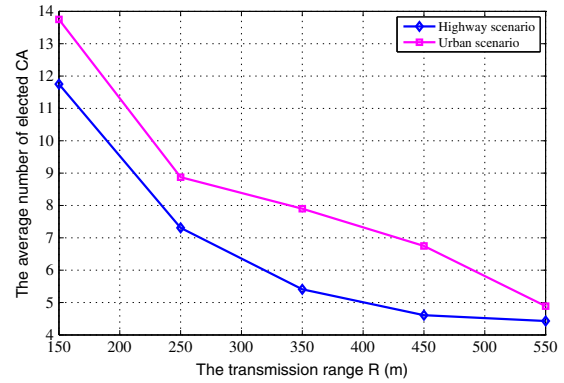


Figure 15. Average number of elected certification authority (CA).

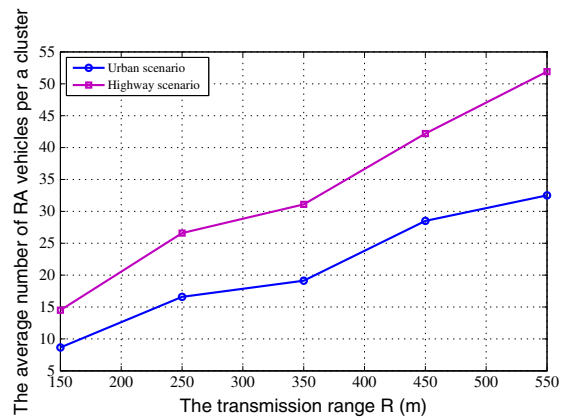


Figure 16. Average number of RA vehicles per one cluster as a function of the transmission range.

represents the urban scenario in Figure 15, we remark that the number of CAs is significantly higher than in highway environment.

To study the average size of the VDDZ, first, we plot in Figure 16 the average number of vehicles RA in a cluster as a function of the transmission range in the case of 100% of vehicles are trusted for both scenarios. We remark that when the transmission range increases, the number of RAs in a cluster raises also. This is an evident behavior of the curves in both urban and highway environments, given that the number of neighbors gets higher when the transmission range is large. This results is confirmed by our analytical results.

Second, we are interested on the consistency of the VDDZ. We plot in Figure 17 the average number of RAs per cluster as a function of the percentage of trusted vehicles in the network. We observe that the number of RAs increases when the number of trusted vehicles increases. In the cases of 5% and 10%, the clusters have an average size of the VDDZ equal to 1 in the urban scenario, which is exactly the sufficient minimal condition to form a cluster. We also observe that the average size of the VDDZ reaches

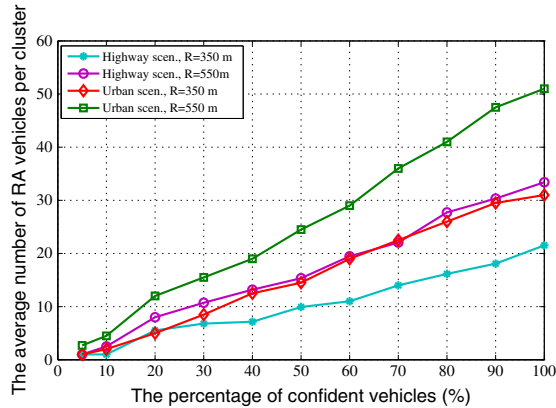


Figure 17. Average number of RA vehicles per one cluster as a function of the percentage of trusted vehicles.

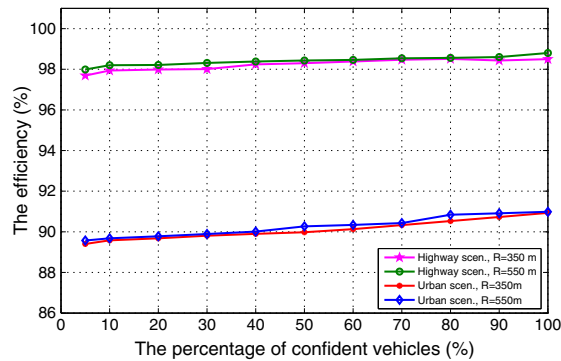


Figure 18. Efficiency of the clustering.

50 RAs per cluster when $R = 550$ m in the urban scenario, which is an important characteristic. Indeed, a large size of the VDDZ guarantees more security for the cluster particularly for its CH. All members of the VDDZ will have an important role in the cluster management as they represent the registration authorities. Further, they play a critical role to establish the anonymity of the CAs as detailed in the previous section.

Let us now study the efficiency of the clustering algorithm. To this purpose, we consider different observation instants, and in each instant, we get the percentage of vehicles attached to clusters the platoon at this instant, this is the instantaneous efficiency. Then, we plot the average of all values of instantaneous efficiency according to the transmission range as shown in Figure 18 for both urban and highway scenarios.

We notice that the efficiency reaches an important value. It is around 90% in the urban scenario and around 98% in the highway scenario. In addition, we remark that the transmission range does not considerably affect the efficiency because if some vehicles do not find a cluster in their neighborhood during a certain period, a new election will take place. Moreover, it is clear that the efficiency in the case of the highway is more significant than in the urban

scenario. In fact, in the urban model, the environment is more dynamic and the vehicles enter and leave the network very quickly. As we described previously, when entering, the network vehicles will have a random destination and a random trajectory.

Thus, there is a probability that the members of a same cluster have different directions at a given instant, which makes vehicles looking for a new cluster for a long time. Furthermore, the efficiency is affected by the cluster life time. In fact, the longer the cluster remains alive, the longer it maintains its members; this makes the architecture stable.

6.2.2. The stability of the clustering.

To study the stability of our clustering algorithm, we focus on the average life time of CA vehicles. To this end, we measure the average time during which a vehicle keeps its status CA relatively to the time that remains to pass in the network. In our algorithm, vehicles can acquire the CA state in the beginning, throughout its trip or in the end. We cannot compare the stability of CA vehicles using only the life time of the vehicle in the state CA because a vehicle can acquire the state CA when it is exiting the network; so, the life time is computed only for a short period. Besides, vehicles have different speeds then, the duration of the trip will be different. That is why we compute the percentage of life time of a CA vehicle relatively to the remained time to pass in the network.

Figure 19 portrays the average life time of CA vehicles as a function of the percentage of trusted vehicles with different transmission ranges in both urban and highway environments.

Let us recall that a vehicle can acquire the role of CA only if it has at least one trusted neighbor to form a VDDZ. Then, the life time of a CA vehicle greatly depends on the number of RA vehicles in its cluster. This is obvious in Figure 19. In fact, the life time of a CA rises when the percentage of trusted vehicles and the transmission range are getting higher. This behavior is related to the variation of the average number of RA vehicles per cluster, which is presented in Figures 16 and 17.

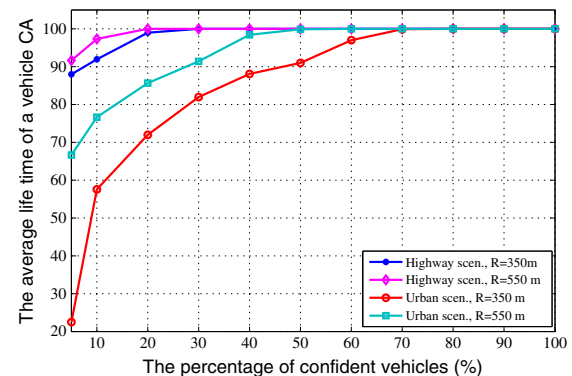


Figure 19. Average life time of a certification authority (CA) vehicle.

As expected in Figure 19, a high number of trusted vehicles and thus, a large size of the VDDZ guarantee a life time of about 100%. It means that if a vehicle is elected CA, it will remain CA until it leaves the network. Furthermore, the life time of a CA is more considerable in the highway model than in the urban model, even if they have approximately the same size of VDDZ (for 10% of trusted vehicles). In addition, even for a large size of the VDDZ in the case of urban model, the life time of the CA is less significant than in the highway model, because the probability to lose all VDDZ members at the same time in the urban model is higher than in the highway model because the vehicles travel in different directions. However, in the highway model, all cars travel towards the same direction.

6.2.3. Evaluating the performances of the certificates management process.

We will investigate three characteristics of our certificates management. The delay required to join a cluster, the delay during which a vehicle last attached to a CA and the average delay of the cross certification.

First, the delay required to join a cluster directly depends on the availability of CA and RA vehicles on the road. Indeed, if there is a sufficient number of CAs to cover the entire network, the time will be reduced to the required time to exchange necessary messages with the correspondent CA to be member of its cluster. Furthermore, if there is a sufficient number of RA vehicles in the VDDZ of a cluster, the detection of a cluster will be faster because as mentioned previously a vehicle detects the presence of a cluster if it receives a HELLO from at least one RA in a VDDZ. Consequently, as depicted in Figure 20, the delay depends on the average number of trusted vehicles in the network, which directly affects the average number of RAs in a VDDZ. We also notice from the plot of Figure 17 that the delay decreases when the average number of trusted vehicles increases. Furthermore, the difference of values between both models is due to the speed; in the highway model, the speed reaches 40 sm/s; however, in the urban model, it only reaches a maximum 20 m/s. Furthermore, a vehicle in the urban model can detect clusters in all

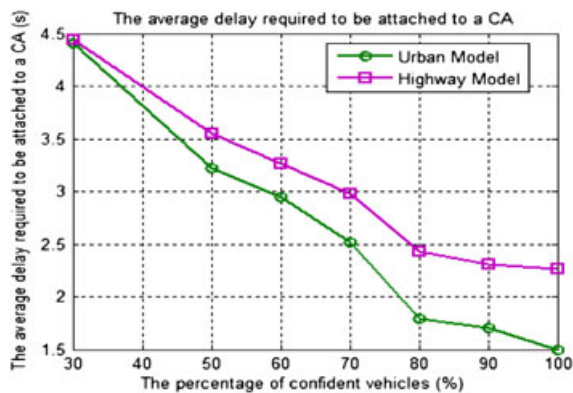


Figure 20. Average delay required to join a cluster.

directions; however, in the highway model, all vehicles travel in the same direction.

Second, we investigate the average delay during which a vehicle still attached to a CH. Figure 21 plots this delay versus the average number of trusted vehicles. Again, a vehicle is still attached to its CH if it periodically receives a HELLO message from its VDDZ (at least one RA). Thus, the delay during which a vehicle becomes member in a cluster depends on the average number of RA vehicles in the VDDZ, which is closely linked to the percentage of trusted vehicles in the network.

Consequently, when the percentage of trusted vehicles increases on the platoon, the average delay during which a vehicle becomes a member of a cluster raises.

In Figure 22, we focus on the cross certification. We plot the average delay required for a cross certification between two CAs as a function of the percentage of trusted vehicles because the more trusted vehicles we have, the more available RA vehicles are to route messages from and to CA vehicles. It also makes the clusters more stable. We consider in VANETs that one vehicle enters the network each

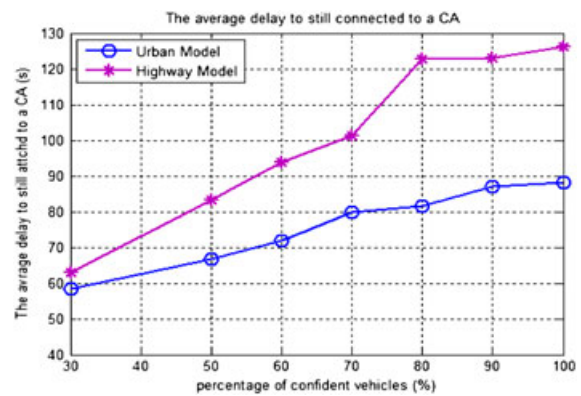


Figure 21. Average delay during which a vehicle still attached to a certification authority (CA).

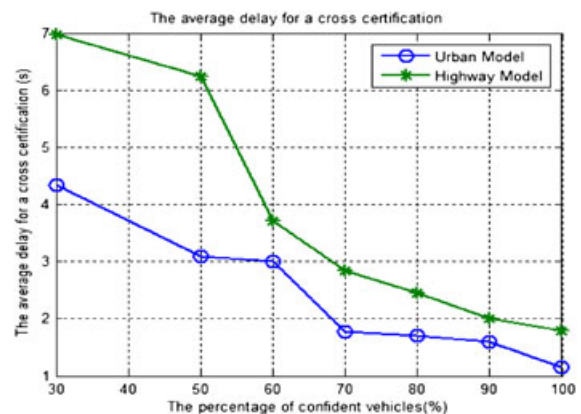


Figure 22. The average delay of a cross certification as a function of the percentage of trusted vehicles.

2 s on average for both scenarios. We consider an event E , which will occur at a time T and a location (x,y) in the network. Once a vehicle detects the event, it broadcasts an alert message in the network.

We remark that the cross certification only lasts some milliseconds, which is efficient for VANETs applications and particularly e-safety applications. We also notice that when the number of trusted vehicles raises, the delay decreases because there are more RA vehicles, which are available to route the message to the CA in less time.

7. DISCUSSION

In this section, we discuss the most important characteristics of the proposed architecture to compare it with other architecture.

First of all, our architecture is fully distributed; the central CA is only intervening in the registration step of vehicles.

In addition, in our work, the presence of RSUs is optional because they have no role neither on the certification process nor on the cross certification compared with [21] and [22] where the RSUs perform those two services. Only vehicles are involved in inter clusters communications.

Also, the role of the CA is distributed among a set of nodes, which avoids the single point of failure. If a CA is compromised, only the certification process of its cluster will be hampered. Furthermore, in the classical distributed PKIs such as in [9], the role of the CA is distributed among nodes without taking into account the stability. The mobility has an important impact on both parameters. Any abrupt variation of the velocity of the CAs can negatively impact the stability of the cluster. Hence, we adapted our clustering algorithm to high speed environments using the relative mobility metric. Unlike [10] where clusters are geographically defined, we elect CA vehicles dynamically according to the topology changes. Our proposed dynamic election guarantees better stability and decreases the number of elected CAs over time. However, it might generate additional overhead compared with their work. Particularly, in our proposal, the architecture is built and maintained using HELLO messages, vehicles must periodically send HELLO during their trip. Furthermore, HELLOs sent by RA vehicles are forwarded up to d hops in each cluster.

Our architecture performs many security services compared with [9,12] and [22] where authors target only specific ones. In fact, the keys and certificates are issued dynamically without storing a large set of keys, also without needing RSUs to request new keys from the central CA. Furthermore, the certificates issued by CAs are short-term to avoid tracking vehicles. In addition, for purpose of anonymity, vehicles generate short-term pairs of key, and they request certificates from the CAs in their clusters. Further, we used the VDDZ to avoid compromising the CA in each cluster and to authenticate unknown vehicles. Unlike the proposal of [9] where any vehicle can sign certificates

for other vehicles, in our clustering algorithm only trusted vehicles can be elected as CH.

8. CONCLUSION

In this paper, we propose a new fully-distributed architecture for certificates management in VANETs. It consists in the establishment of a distributed PKI based on an adequate trust model and on an efficient clustering algorithm.

To enhance the security of CAs, we proposed to protect them from any direct communication with unknown vehicles. To this goal, we introduced a new concept of VDDZ. Its role is to protect the CA in the cluster by preventing any direct communication between the CA and unknown vehicles requesting a certificate from the CA. Besides, we propose a connectivity model to study the robustness of the VDDZ in the clusters. We also demonstrated how to perform secured and anonymous communications within various VANET applications (unicast and broadcast).

The simulation results show that our clustering algorithm elects a minimal number of CA vehicles to cover the entire network. In addition, the stability of the clustering algorithm strongly depends on the transmission range and the percentage of trusted vehicles in the network. Also, the clustering algorithm is more efficient and stable in the highway model than in the urban scenario. As shown by the analytical results, one important factor that has an important impact on the deployment of our architecture is V2V connectivity.

One possible drawback of our proposal is the generated overhead because of the HELLO messages used to establish and maintain the architecture. The network overhead might be optimized to avoid frequent collisions and congestion mainly when data traffic is injected in the network.

In our future work, we are focusing on the trust model and the revocation of malicious vehicles within the proposed PKI. Furthermore, we plan to work on comparing our proposed architecture with other related works.

REFERENCES

1. The Intelligent Transportation Systems Committee. *IEEE P1609.0 Draft Standard for Wireless Access in Vehicular Environment (WAVE)-Architecture*, January 2009.
2. IEEE 802.11 Working Group of the IEEE 802 Committee. *IEEE P802.11p/D5.0 Draft Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless Access in Vehicular Environments (WAVE)*, November 2008.

3. The Intelligent Transportation Systems Committee. *IEEE P1609.1 Draft Standard for Wireless Access in Vehicular Environments WAVE Resource Manager*, November 2005.
4. The Intelligent Transportation Systems Committee. *IEEE P1609.2 Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, November 2005.
5. The Intelligent Transportation Systems Committee. *IEEE P1609.3 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services*, December 2008.
6. The Intelligent Transportation Systems Committee. *IEEE P1609.4 IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Multichannel Operation*, November 2006.
7. Mishra B, Nayak P, Behera S, Jena D. Security in vehicular adhoc networks: a survey. *Proceedings of the 2011 International Conference on Communication, Computing and Security: ICCCS 11*, Rourkela Odisha India, 2011, February 2011; 590–595.
8. Parno B, Perrig A. Challenges in securing vehicular networks. *Proceeding of the Workshop on Hot Topics in Networks (HotNets-IV)*, Maryland, 2005.
9. Sivagurunathan S, Subathra P, Mohan V, Ramaraj N. Authentic vehicular environment using a cluster based key management. *European Journal of Scientific Research ISSN 2009*; **36**(2): 299–307.
10. Raya M, Paradimitratos P, Hubaux JP. Securing vehicular communications. *IEEE Wireless Communications* 2006; **13**(5): 8–15.
11. Park S, Aslam B, Zou C. Long-term reputation system for vehicular networking based on vehicles daily commute routine. *IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, 2011; 436–441.
12. Blum J, Eskandarian A. The threat of intelligent collisions. *IT Professional* 2004; **6**(1): 24–29.
13. Gazdar T, BenSlimane A, Belghith A. Secure clustering scheme based keys management in VANETs. *The IEEE 73rd Vehicular Technology Conference (VTC2011)*, Budapest, Hungary, 2011; 1–5.
14. Krajzewicz D, Hertkorn G, Wagner P, Rössel C. SUMO (Simulation of Urban Mobility): an open-source traffic simulation. *Proceedings of the 4th Middle East Symposium on Simulation and Modelling: MESM2002*, Sharjah, United Arab Emirates, 2002.
15. Papadimitratos P, Gligor V, Hubaux JP. Securing vehicular communications - assumptions, requirements, and principles. *4th Workshop on Embedded Security in Cars*, 14–15 November 2006, Berlin.
16. Leinmueller T, Buttyan L, Hubaux JP, Kargl F, Kroh R, Papadimitratos P, Raya M, Schoch E. SEVECOM secure vehicle communication. *IST Mobile and Wireless Communication Summit (MobileSummit'2006)*, Mykonos, Greece, 2006.
17. Youl Choi J, Jakobsson M, Wetzel S. Balancing auditability and privacy in vehicular networks. *Q2SWinet05*, Montreal, Quebec, Canada, 2005; 79–87.
18. Wasef A, Shen X. PPGCV: privacy preserving group communications protocol for vehicular ad hoc networks. *Proceedings of IEEE International Conference on Communications: ICC 2008*, Beijing, China, 2008; 1458–1463.
19. Perrig A, Canneti R, Song D, Tygar JD. The TESLA broadcast authentication protocol. *RSA Cryptobytes* 2002; **5**(2): 2–13.
20. Pei-Yuan S, Vicky L, Maolin T, Caelli W. An efficient public key management system: an application in vehicular ad hoc networks. *Pacific Asia Conference on Information Systems (PACIS)*, Brisbane, Australia, 2011.
21. Coronado ES, Cherkaoui S. Performance analysis of secure on-demand services for wireless vehicular networks. *Security and Communication Networks Journal* 2010; **3**(2–3): 114–129.
22. Hesham A, AbdelHamid A, Abou ElNasr M. A dynamic key distribution protocol for PKI-based VANETs. *IFIP Wireless Days 2011*, Niagara Falls, Ontario, Canada, October 10–12, 2011; 1–3.
23. Little TDC, Agrawal A. An information propagation scheme for VANETs. *Proceedings of the 8th International IEEE Conference on Intelligent Transportation Systems (ITSC2005)*, Vienna Austria, 2005; 155–160.
24. Raya M, Aziz A, Hubaux JP. Efficient secure aggregation in VANETs. *VANET '06 Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, Los Angeles, California, USA, 2006; 67–75.
25. Luo Y, Zhang W, Hu Y. A new cluster-based routing protocol in VANET. *Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing: NSWCTC '10*, Vol. 1, Wuhan, China, 2010; 176–180.
26. Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K. CARAVAN: providing location privacy for VANET. *Proceedings of the Workshop on Embedded Security in Cars (ESCAR)*, Cologne, Germany, 2005.
27. Fan P, Haran G, Dillenburg J, Nelson P. Cluster-based framework in vehicular ad-hoc networks. *4th International Conference, ADHOC-NOW 2005*, Cancun, Mexico, October 6–8, 2005; 32–42.

28. Jiang M, Li J, Tay YC. Cluster based routing protocol. *IETF Draft*, August 1999.
29. Krishna P, Vaidya NH, Chatterjee M, Pradhan DK. A cluster based approach for routing in ad hoc networks. *Proceedings of the 2nd Symposium on Mobile and Location-Independent Computing (MLICS'95)*, Ann Arbor, MI, USA, 1995.
30. Wang Z, Liu L, Zhou M, Ansari N. A position-based clustering technique for ad hoc inter vehicle communication. *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews* 2008; **38**(2): 201–208.
31. Goonewardene RT, Ali FH, Stipidis E. Robust mobility adaptive clustering scheme with support for geographic routing for vehicular ad hoc networks. *IET Intelligent Transport Systems* 2009; **3**(2): 148–158.
32. Rachedi A, Benslimane A. A secure and resistant architecture against attacks for mobile ad hoc networks. *Security and Communication Networks* 2010; **3**(2–3): 150–166.
33. Marmol F, Perez G. TRIP: a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications* 2012; **35**(3): 934–941.
34. Tajeddine A, Kayssi A, Chehab A. A privacy-preserving trust model for VANETs. *International Conference on Computer and Information Technology*, China, 2010; 832–837.
35. Govindan K, Mohapatra P. Trust computations and trust dynamics in mobile ad hoc networks: a survey. *IEEE Communications Surveys Tutorials* 2011; **PP**(99): 1–20.
36. Gazdar T, Rachedi A, BenSlimane A, Belghith A. A distributed advanced analytical trust model for-VANETs. *IEEE Global Communications Conference (GLOBECOM'12)*, Anaheim, California, USA, 2012.
37. Kumar U, Helmy A. Proximity-based trust-advisor using encounters. *ACM SIGMOBILE Mobile Computing and Communications Review* 2010; **14**(4): 22–24.
38. Taleb T, Benslimane A, Benletaief K. Toward an effective risk-conscious and collaborative vehicular collision avoidance system. *IEEE Transactions on Vehicular Technology* 2010; **59**(3): 1474–1486.
39. Ma X, Chen X, Refai H. Performance and reliability of DSRC vehicular safety communication: a formal Analysis. *EURASIP Journal on Wireless Communications and Networking* 2009; **2009**(3).
40. Kafsi M, Papadimitratos P, Doussey O, Alpcanz T, Hubaux JP. VANET connectivity analysis. *IEEE Workshop on Automotive Networking and Applications (AUTONET)*, New Orleans, LA, USA, 2008.
41. Vargas A. The OMNeT++ discrete event simulation system. *Proceedings of the European Simulation Multiconference ((ESM))*, Czech Republic, June 6–9, 2001.
42. Al-Doori M. Directional routing techniques in VANET. *Ph.D. Thesis*, November 2011.
43. Khan I, Qayyum A. Performance evaluation of AODV and OLSR in highly fading vehicular ad hoc network environments. *IEEE 13th International Multitopic Conference(INMIC 2009)*, Islamabad, Pakistan, 2009.