An Adaptive Key Exchange Procedure for VANET

Hamza Toulni
GITIL Laboratory, LIAD. Faculty of Sciences Aïn Chock
Hassan II University of Casablanca
Casablanca, Morocco

Benayad Nsiri
GITIL Laboratory, LIAD. Faculty of Sciences Aïn Chock
Hassan II University of Casablanca
Casablanca, Morocco

Mohcine Boudhane
GITIL Laboratory, LIAD. Faculty of Sciences Aïn Chock
Hassan II University of Casablanca
Casablanca, Morocco

Mounia Miyara
LIAD Laboratory. Faculty of Sciences Aïn Chock
Hassan II University of Casablanca
Casablanca, Morocco

***Abstract*—VANET is a promising technology for intelligent transport systems (ITS). It offers new opportunities aiming at improving the circulation of vehicles on the roads and improving road safety. However, vehicles are interconnected by wireless links and without using any infrastructure, which exposes the vehicular network to many attacks. This paper presents a new solution for the exchange of security keys to protect information exchanged between vehicles. In addition to securing the inter-vehicular communication, the proposed solution has considerably decreased the time for the exchange of keys, thus improving the performance of VANET.**

Keywords—ITS; Vehicular ad-hoc networks; public key exchange; Security

I. Introduction

Vehicular Ad Hoc NETworks (VANETs) are a wireless communication technology applied to transportation; it is specially designed to solve the problems caused by the increasing number of vehicles and urban sprawl. VANET permits communication between vehicles themselves or between vehicles and the road infrastructure to improve the intelligent transport systems by the major benefits that can be gained from wireless technology, such as the improvement of road safety and traffic fluidity.

VANET is a subclass of MANET (Mobile Ad Hoc Networks), in which the mobile nodes are replaced by vehicles. So vehicles inheriting all properties associated with the nodes in MANET, but with some special characteristics, such as high speed of nodes which makes the environment of VANET highly dynamic, and this leads to frequent network topology changes. And unlike traditional wireless networks where limited power is a major constraint, nodes of vehicular networks have large capacities of energy they derive from vehicle power system, which ensures better performance in the computations.

However, in addition to the problems inherited from MANET, there are other challenges [1] that must be overcome to enable communication between vehicles by VANET. One of the most critical and important problems is security and privacy, due to the importance of information exchanged within VANET, and each change in the alerts constitutes a serious threat to people's lives.

VANET is an ideal target for various attacks [2] because vehicles share among themselves all kinds of information via wireless links without any administration by a centralized infrastructure, this facilitates attackers to intercept the information exchanged or to inject wrong information in the network. Hence the importance of securing VANET to protect the exchanged information, but adding the security mechanism involves an additional computation cost in the network, thereby influencing the transmission performance.

To address this critical issue of security, a new procedure for the exchange of security keys is present in this paper to protect information exchanged between vehicles, in addition to ensuring the inter-vehicle communication; the proposed solution has significantly reduced the time for key exchange, improving the performance of VANET.

The rest of the paper is organized as follows; the following section provides an overview of security in VANET. In Section III, we present an overview of cryptography. In Section IV, we present the proposed key exchange procedure. In Section V, we present the simulation results and an analysis of the proposed procedure. Finally, we conclude the paper in Section VI.

II. Related Work

VANET is a promising technology that provides several advantages to supply value added services to improve safety and traffic, but the nature of the transmission medium makes VANET more vulnerable to attack. Therefore, network security is an essential element to support the implementation and operation of applications and services in VANET.

A. *The security threats*

As each network VANET is exposed to several attacks:

- Sniffing: The malicious vehicles listening to the transmission medium in order to extract information exchanged in its neighborhood; it may want to spy on personal information or collect information and to perform then other types of attacks.
- Unauthorized access: The malicious vehicles are accessing to network services without having the rights or privileges.

- Denial of Service: The goal is to make the different resources and services unavailable to users in the network; it is usually caused by other attacks on the bandwidth or energy resources of other nodes. The most naive technique to cause a denial of service in a wireless network is Jamming, another method of attack which consists of requesting a service that provides by a node in a repetitive manner in order to waste his resources.

- Spoofing: The malicious vehicles attempting to impersonate another node in order to receive their messages or have the privileges that are not granted.

- Falsifying information: Malicious vehicles are attempting to change the information contained in a message or even remove messages during their trip.

- Therefore, the security mechanisms in VANET must necessarily reach a number of general security requirements, such as:

- Authentication: This security required allows network members to ensure the correct identification of vehicles with which they communicate, and thus know more information about the issuer vehicle as its identifier, address, properties, and its geographical position.

- Integrity: This security required helps to ensure that the data exchanged are not subjected to voluntary or accidental tampering. Thus, it allows recipients to detect data manipulation by unauthorized entities and to reject the packages.

- Confidentiality: This security required guarantees that only authorized entities can access to data transmitted across the network. However, the confidentiality of information in VANET depends on the application and the communication scenario, especially in the case of warning messages of an emergency that must be read by any entity in VANET.

- Non-repudiation: This security required ensures that no required sender cannot deny being at the origin of a message, this objective is essential in sensitive communications. So the overall purpose of non-repudiation is to collect, maintain and make available all the evidence about an event or action, to resolve disputes about an occurrence and not an action. Non-repudiation depends on authentication, and the system can identify the author of a malicious message.

- Availability: This security is required to guarantee entities authorized to access network resources with adequate quality of service. The resources must remain available even in the case of failure in the network. This not only secures the system but also makes it fault tolerant. And resources should remain available until the fault is repaired.

To satisfy these requirements and overcome the threats of attacks, many researchers have proposed solutions to ensure secure communication within VANET.

B. *Proposed solutions*

In the literature, the security issue VANET attracted the attention of many researchers, and several solutions have been proposed to overcome the threats of attacks.

In [3] Raya, *et al.* propose a detailed analysis of threats that endanger VANET and propose a security architecture. This architecture is based on the use of private keys and also included a certification authority, they also proposed a method for the management and conservations of the keys.

In [4], Karl, *et al.* have proposed the Security-Requirements Engineering using Cluster Analysis (SECA). This is an approach which allows the analysis of a large number of applications by selecting a typical representation covering the required application cluster, then, they determine the security mechanisms for all subsets of trained applications.

In [5], Plossl, *et al.* have proposed a security architecture for VANET (SAV). The communication model of this architecture is based on the fact that there are two types of communication: communication messages passive such as beacons messages that are sent periodically and active communication messages that are sent when an event occurs and a warning is to be sent to neighboring vehicles. The security architecture they propose for VANET is divided into three layers: The lower layer that includes basic security features, The security layer to jump, and The multi-hop layer, it includes all the applications and services used in VANET.

In [6] Dhurandhar, *et al.* have presented Vehicular Security through Reputation and Plausibility checks (VSRP) approach to deploy security in VANET, their algorithms take into account three types of events: traffic jams, accidents, and braking applications. The algorithm uses a system based on the reputation of the sensors, not only to detect but also to isolate malicious nodes present in the network. This algorithm also allows managing the problems related to aggregation and deletion of data. This algorithm operates on an event-oriented approach. Three types of events are listed: a-jumping, multi-jump, and malicious intent. The protocol distinguishes three types of packages for messages: data packets, requests packets of neighbors (neighborreq packet), and response packets neighbors (neighborrep packet).

In [7] Golle, *et al.* proposed a general approach to assessing the validity of data in the VANET. In their approach, the node tries different possible explanations about the data it has collected; based on the assumption that a malicious node is afraid to attend. Their techniques to assess and classify the nodes depends on two assumptions: the nodes have an ability to exchange information with each other, plus a parsimony argument accurately reflects contradictory behavior in the VANET. This technique allows them to detect incorrect information about the identity of the node or nodes of the emitters of this incorrect information with high probability.

In [8], Tiffany Hyun-Jin, *et al.* proposed a model to distinguish spurious messages from legitimate messages. They explore six different sources of information to enable vehicles to filter malicious messages that are transmitted by a minority of disobedient vehicles. The six sources are as follows.

- The digital signature verification result.
- The geographical location of the source.
- Local sensors to the vehicle.
- The messages of other vehicles: Is there a contradiction between alerts?
- The validation infrastructure (RSU).
- The reputation of the issuer.

This model validation warning is based on two components: the level and the Certainty of Event (CoE). An alert is triggered when the certainty of the event exceeds a threshold.

III. Cryptography

Security is an unsurpassable prerequisite for the deployment of VANET. In fact, wireless networks are generally vulnerable to espionage and attacks, and the importance of information sent between vehicles, increase the probability of occurrence of these threats.

Cryptography is the technique used to make the confidential data by encrypting at the source node and deciphering at the destination node. It can be considered as a key solution to most of these threats.

We distinguish two types of encryption and decryption algorithms [9].

- Symmetric-key algorithms in which all nodes have the same encryption key.
- Asymmetric-key algorithms where we distinguish the use of two keys, one public known by all nodes and the other is private for each node.

To ensure that the information is only accessible by authorized entities, the most reliable solution is to use asymmetric algorithms. This infrastructure is known As Public Key Infrastructure (PKI).

In a PKI, the communication is encrypted with a digital certificate and obtain this certificate, the entity made a request to the Registration Authority. This generates a couple of keys (public key, private key) and sends the private key to the entity. Consequently, PKI communication takes place in several phases as shown in Figure 1.

- *Phase 1*: the entity B requests access to entity A.
- *Phase 2:* the entity A sends its certificate, which contains its public key.
- *Phase 3:* the entity B verifies the authenticity of the certificate of entity A. Specifically, it checks the signature of entity A. At this moment, the entity B is sure of the authenticity of the certificate of the entity A
- *Phase 4:* same as phase 2, the entity B sends its certificate.
- *Phase 5:* same as phase 3, the entity A verifies the certificate of entity B. At this time, the A entity is sure of the authenticity of the certificate of the entity B
- *Phase 6:* the entity A sends a message unencrypted randomly generated to entity B.
- *Phase 7:* the entity B encrypts the received message using its private key and sends it. The entity A decrypts the message using the public key of the entity B. At that moment the entity A is sure about the identity of entity B.
- *Phase 8:* same as phase 6, but in the other direction. The entity B sends a message unencrypted randomly generated to entity A.
- *Phase 9:* same as phase 7, but in the other direction. At this moment, the entity B is sure of the identity of the entity A
- *Phase 10:* exchange of information between the entity A and the entity B can be started in complete securely.

However, in VANET, the use of traditional PKI phases is a challenge because of the constraints the response time and the architecture of this network. However, the characteristics and requirements of applications and services require the definition of specific protocols.

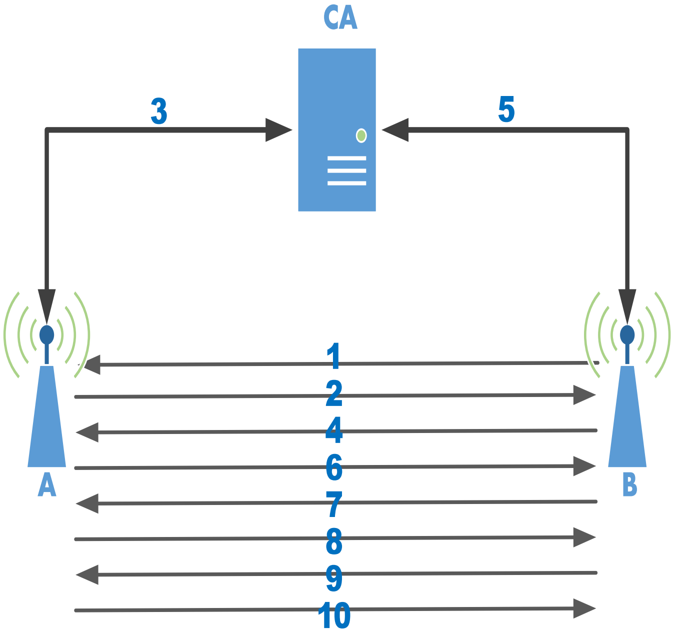

Fig. 1. Key exchange mechanism in the Public Key Infrastructure

IV. The Proposed Procedure

Due to high-speed vehicles, minimizing the end-to-end delay in VANET is highly importance to ensure the proper functioning of services and applications while satisfying the requirements of security in this type of network. However, using traditional security mechanisms cause negative effects on the quality of services and applications because these mechanisms are complex and require a lot of time which leads to additional delays for the information to reach its destination even if the energy, memory, and computational capacity do not constitute any obstacle in VANET.

To remedy this problem, we propose a new procedure for the exchange of security keys while respecting the requirements of communication in VANET. So for this proposal, we assume that all of the vehicles are grouped into clusters as shown in Figure 2, and each cluster has only one manager node (Cluster Head). This Cluster Head will be responsible for vehicle integration and validation of the security keys.

In the rest of this paper, we use the following notation to describe the proposed procedure.

TABLE I. NOTATION AND SYMBOLS USED

Symbol	*Description*
CA	Certification Authorities
PK_i	The public key of a vehicle i.
SK_i	The private key of a vehicle i.
E(k,M)	The encrypted message M with the key k.
V_R	Random value.
H()	The hash function.

A. Cluster Schema

As previously mentioned, the network is divided into clusters as shown in Figure 2. The aim of the cluster is to maximize the lifetime of connections between vehicles, for this, the cluster creation is based primarily on two criteria: the direction and average speed of vehicles. Thus, the cluster has at least one member vehicle and at most one cluster Head. This Cluster Head will assume the role of Certification Authorities (CA).

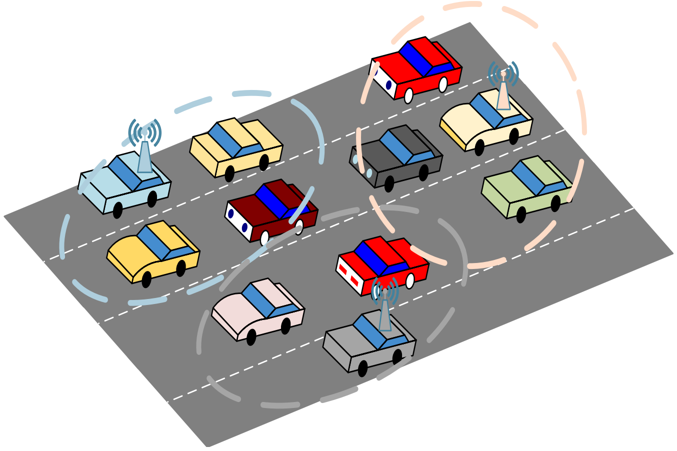

Fig. 2. The formation of clusters

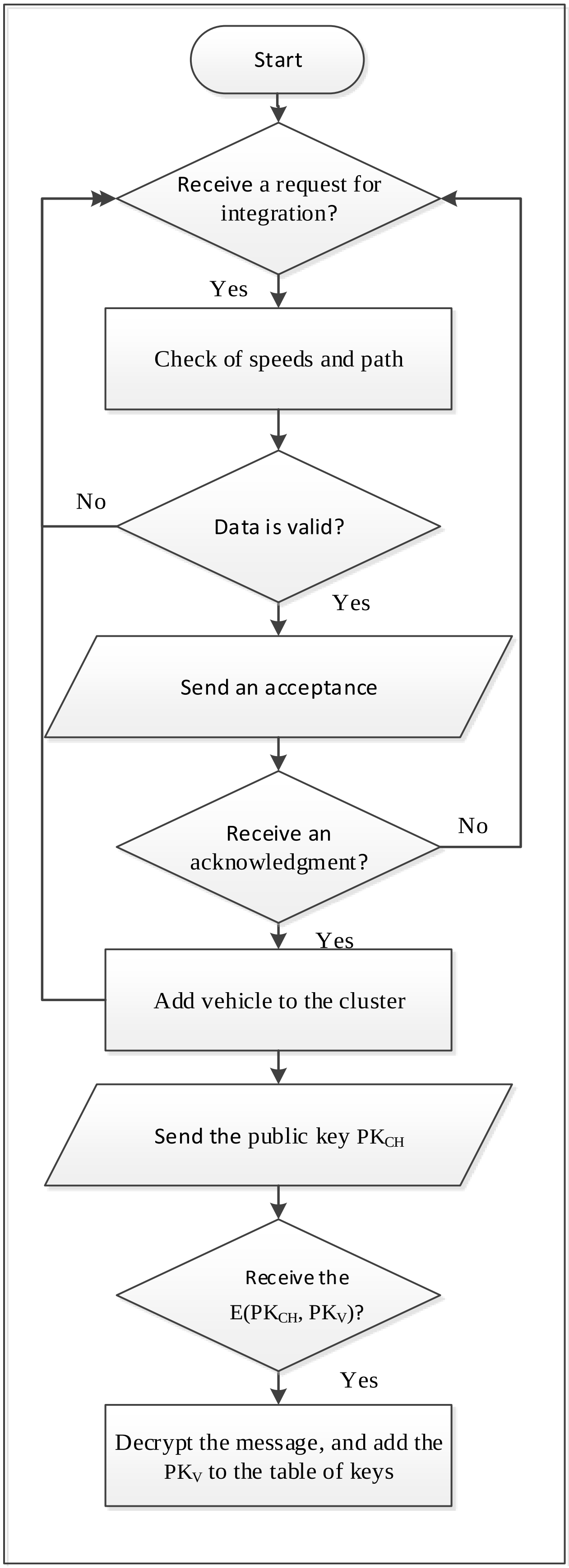
Start
Receive a request for integration?
Yes
Check of speeds and path
No
Data is valid?
Yes
Send an acceptance
Receive an acknowledgment?
No
Yes
Add vehicle to the cluster
Send the public key PK_{CH}
Receive the $E(PK_{CH}, PK_V)$?
Yes
Decrypt the message, and add the PK_V to the table of keys

Fig. 3. The integration of a vehicle in the cluster

If the cluster is not yet formally established, and there are at least two vehicles, first, these vehicles will be a check of their speeds and path, the path is the common route segment between vehicles that should be sufficiently long to establish a connection and exchange information, the speed should be around of average speed of the other vehicles so that the vehicle remains in communication with the other vehicles of the same cluster, and the Cluster Head is elected according to its path that must be the longest path on the road compared to other cluster members.

On the other hand, if the cluster is already created, the vehicle broadcasts a request for integration with its speed and path and subsequently, the Cluster Head receives the request as shown in Figure 3. Then, they check the speed and around average speed of the cluster and the road segment in common between the vehicle and the Cluster Head is long enough, whether the Cluster Head sends an acceptance and waits for an acknowledgment. Once the vehicle is integrated into the cluster, the Cluster Head sends its certificate, which contains its public key PK_{CH}, and the vehicle sends $E(PK_{CH}, PK_V)$ to Cluster Head, which represents the public key PK_V encrypted using the public key of the Cluster Head PK_{CH}, the Cluster Head decrypts the message with his private key SK_{CH} and add the PK_V to the table of keys in its database.

B. *The exchange of keys between cluster members*

The exchange of public keys between the cluster members in the proposed procedure involves three entities.

- The initiator vehicle A
- The responder vehicle B
- The Cluster Head.

Both vehicles A and B are members of the same cluster, so the two vehicles are already identified at the Cluster Head, which owns their public keys.

The sharing of keys applies only to the vehicles A and B, and not the other cluster members, but once the share is finished the keys are stored in the vehicles A and B, which decreased considerably in the exchange of useless messages between vehicles, and thus improves network performance while ensuring the security of the communication.

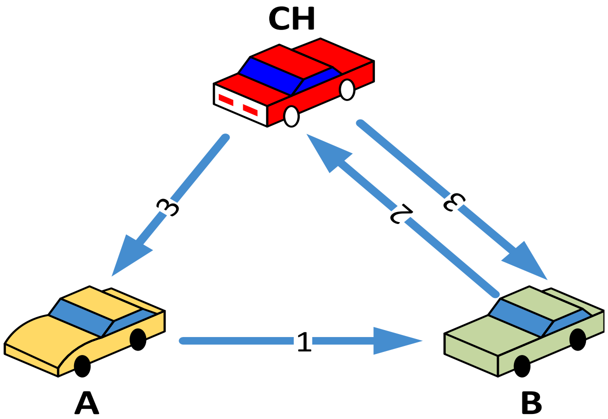

Fig. 4. Exchange public keys between cluster members

The proposed procedure will be conducted in three main phases as shown in Figure 4.

- ***Phase 1***: The vehicle initiator A sends a request to establish communication with the vehicle B. This request contains:
  - The identifier of the vehicle A.
  - A random value V_R generated by A, this value is randomly generated and different for each request of establishing communication.
  - $E(SK_A, V_R)$ the encryption of V_R with the private key SK_A of vehicle A.
  - $H(V_R|E(SK_A, V_R))$ the hash of the V_R and $E(SK_A, V_R)$.
- ***Phase 2***: The vehicle B build its own request to the Cluster Head, which contains:
  - The identifier of the vehicle A.
  - $E(SK_A, V_R)$ the encrypted message sent by the vehicle A.
  - $H(ID_A|E(SK_A, V_R))$ the hash of the V_R and the identifier of the vehicle A.
- ***Phase 3***: The Cluster Head build two messages the one for the vehicle A and the other for the vehicle B, the first message contains:
  - $E(SK_{CH}, PK_B)$ the encryption of the public key PK_B of vehicle B with the private key SK_{CH} of Cluster Head.
  - $E(SK_{CH}, V_R)$ the encryption of V_R with the private key SK_{CH} of Cluster Head.
  - $H(E(SK_{CH}, PK_B)|E(SK_{CH}, V_R))$ the hash of the encrypted PK_B and the encrypted V_R.

And the second message contains:

- $E(SK_{CH}, PK_A)$ the encryption of the public key PK_A of vehicle A with the private key SK_{CH} of Cluster Head.
- $E(SK_{CH}, V_R)$ the encryption of V_R with the private key SK_{CH} of Cluster Head.
- $H(E(SK_{CH}, PK_A)|E(SK_{CH}, V_R))$ the hash of the encrypted PK_A and the encrypted V_R.

V. Simulation and Analysis

A. *Simulation*

We choose SUMO (Simulation of Urban MObility) and NS2 (Network Simulator 2) as a simulation platform, in order to test the effectiveness of the proposed procedure. SUMO is designed to manage large real route maps, which can be downloaded from OpenStreetMap, which allow to simulate different scenarios in different parts of the world. SUMO has the ability to operate as a server and to report the simulation data in real time NS2.

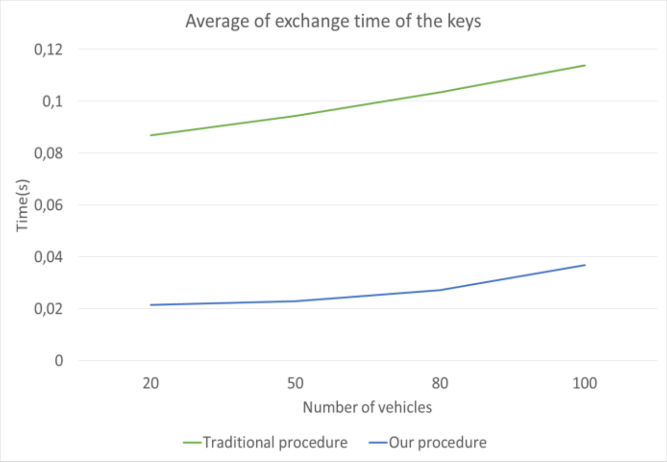

Fig. 5. Exchange public keys between cluster members

SUMO allows the changing of simulation scenarios in NS2 at runtime and thereby provide a dynamic simulation in NS2, and highlight the effectiveness of the proposed procedure.

The purpose of this simulation is to compare the performance of the proposed procedure with the traditional public key exchange procedure. For this, we consider multiple scenarios depending on the number of vehicles, and in each scenario, we randomly selected the path of each vehicle in different places on the map. We used same scenarios for both procedures; we use the following simulation parameters:

TABLE II. SIMULATION PARAMETERS

Map size	1500m x 1500m
Number of vehicles	20,50,80,100
Average speed	15m/s
Simulation time	900s
MAC protocols	IEEE 802.11p
Routing protocols	AODV
Hash function	SHA-1

For both the procedures, and for each scenario, we calculate the average of the exchange time of the keys between vehicles collected during execution.

In Figure 5 which illustrates the results of the simulation, we note that, if the network size increases, with more vehicles, the exchange time of the keys increases slightly in both the procedures. However, the exchange time in the proposed procedure is lower than the time spent in the traditional procedure.

Therefore, the proposed procedure shows a better performance in comparison with the traditional procedure, as the proposed procedure is achieved with only three phases, versus ten phases in the traditional procedure.

Therefore, the proposed procedure can significantly reduce the time to establish a secure communication between vehicles, thus improving the performance of VANET.

B. Security Analysis

The proposed procedure aims to secure the inter-vehicle communication, and thus ensures:

Authentication which consists of verifying the vehicle identity. In the proposed procedure, each vehicle stores an identifier and a pair of keys for secure communication. The signature of each message distributed by the private key provides the authentication of each number.

Integrity, which consists of verifying the integrity of the message when it's exchanged, and not subjected to voluntary or accidental tampering. In the proposed procedure, it is assured by a hash function, which is irreversible.

Confidentiality guarantees that only legitimate message recipient can read it. Therefore, encryption with a public key and decrypted with the private key in the case of receiving the message, and the case of sending encryption messages with the private key and the deciphering with the public key.

Non-repudiation is a much-desired property in VANET because the nature of VANET easily enables you to listen or disrupt the messages exchanged. The attacker can make a replay attack, it is a type of man in the middle attack that consists of intercepting the message and the retransmitted later. Non-repudiation depends on authentication, but the replay attack cannot be confronted by authentication and integrity only. That's why in each request a different random number is generated and included in the request to prevent this type of vulnerability.

VI. CONCLUSION

VANET is a promising technology for the intelligent transportation system. VANET is a promising technology for the intelligent transportation system. However, VANET has many constraints such as the fast moving of vehicles and collective communication medium without any administration by a centralized infrastructure, these constraints combine to make the difficult and complex VANET security to apprehend, and this makes VANET an ideal target for different attacks.

In this paper, a new solution for the exchange of security keys is presented in order to protect information exchanged between vehicles. The proposed procedure can reduce significantly, the delivery time and secure communication and improve VANET performance at the same time.

The proposed procedure is simulated and it has been compared with the traditional procedure keys exchange in several conditions, the experimental result shows that the proposed procedure is very effective. In the future work, we will try to improve the proposed procedure by adding more complexity in different attacks.

REFERENCES

[1] Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Yunchuan Sun, and Rongfang Bie. "Vehicular Ad Hoc Networks: Architectures, Research Issues, Challenges and Trends." In Wireless Algorithms, Systems, and Applications, pp. 102-113. Springer International Publishing, 2014.

[2] Sumra, I.A.; Bin Hasbullah, H.; Bin AbManan, J.-L., "Effects of attackers and attacks on availability requirement in vehicular network: A survey," in Computer and Information Sciences (ICCOINS), 2014 International Conference on , vol., no., pp.1-6, 3-5 June 2014.

[3] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[4] Kargl Frank, Zhendong Ma, and Elmar Schoch. "Security engineering for VANETs." Proc. 4th Wksp. Embedded Sec. in Cars, pp.15-22, 2006.

[5] Plossl, K.; Nowey, T.; Mletzko, C., "Towards a security architecture for vehicular ad hoc networks," in The First International Conference on Availability, Reliability and Security, 2006. ARES 2006., pp.8 pp.-, 20-22 April 2006

[6] Dhurandher, S.K.; Obaidat, M.S.; Jaiswal, A.; Tiwari, A.; Tyagi, A., "Securing vehicular networks: A reputation and plausibility checks-based approach," in GLOBECOM Workshops (GC Wkshps), 2010 IEEE , vol., no., pp.1550-1554, 6-10 Dec. 2010

[7] P. Golle, D. Greene and J. Staddon, Detecting and correcting malicious data in VANETs, in: Proceedings of VANET'04, 2004, pp. 29–37.

[8] Tiffany Hyun-Jin Kim, Ahren Studer, Rituik Dubey, Xin Zhang, Adrian Perrig, Fan Bai, Bhargav Bellur, and Aravind Iyer. “VANET alert endorsement using multi-source filters”. In Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking (VANET '10). ACM, New York, NY, USA, 51-60. 2010.

[9] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. " Handbook of Applied Cryptography". CRC press series on Discrete mathematics and its Applications. CRC Press 1997.