Securing Southbound Interface of HSDN-GRA Vehicular Routing Protocol using a Distributed Trust

Lylia Alouache
Ferhat Abbas University Setif1
Universit Paris Seine,EISTI,ENSEA,CNRS
ETIS,UMR8051// LRSD
Algeria, France
lae@eisti.eu

Mohamed Maachaoui
Computer science departement//EISTI
Quartz
Paris, France
mmaa@eisti.eu

Makhlouf Aliouat
Ferhat Abbas University Setif1
Computer Science departement LRSD
Setif, Algeria
maliouat@univ-setif.dz

Rachid Chelouah
Computer science departement//EISTI
ETIS,UMR8051
Paris, France
rc@eisti.eu

***Abstract*—The progress of wireless technologies in recent years has tipped the automotive industry towards the digital world with multiple communication systems forming Internet of Vehicles (IoV). These communication systems are subject to disturbances and alterations due to the wireless and dynamic characteristics of vehicles. IoV aims to integrate new information services, safety applications, and internet services, based on the benefits of cloud computing, It tries to improve safety and comfort on the road. The deployment of these services requires messages to be exchanged between the vehicles in a secure manner. Consequently, routing and security topics are crucial to provide a quality of services and to preserve the data integrity. The Software Defined Networking (SDN) architecture is the way that can guarantee these two issues. The purpose of this paper is, firstly, to present the impact of SDN architecture in a vehicular network. Besides, as the robustness of the routing protocols depends on the integrity and authenticity of the routing rules, an improvement of the HSDN-GRA vehicular routing protocol is also described. This improvement develops a distributed trust model and aims to secure the communication between the control plane and the data plane. The goal is to secure the southbound interface between the defined semi-centralized controller and the other vehicles, as well as the Vehicle to Vehicle (V2V) communication.**

***Index Terms*—IoV, V2V, SDN, Communication, Routing protocols, Availability, Reliability, QoS, Security, Integrity, Trust.**

I. Introduction

The high mobility and the low density of vehicles results in frequent network partitioning, unconnected network and isolated vehicles. The known traditional ad-hoc architecture on which the IoV's ancestor is based, called the Vehicular Ad-Hoc Network (VANET), suffers from many lacks such as frequent disconnections due to the high mobility of the nodes, high communication delays due to the multi-hop scenarios, and very limited security because of the different attacks and intrusions against the wireless and the heterogeneous network. The most known are: Sybil attack, Black hole attack, Replay attack, Denial of Services attack, position attack etc. [1] [2] [3]. To overcome these challenges ranging from data routes management to data security and user privacy, the Software Defined Networking (SDN) paradigm has been identified as a suitable approach for dealing with: the dynamic network environment, the increased number of vehicles, the quality of communication, the heterogeneity of the applications and the communication technologies, the routing strategies and the security issues [4]. The SDN architecture is designed by disassociating the control plane from the data plane. The first one makes decisions about where data is sent while the second forwards data to the selected destination according to the control plane rules. Some investigations have been conducted in recent literature about the applicability of the SDN for vehicular network communications [2] [5] [6] [7] [8] [9] [10] [11] [12] [13] frequently called Software Defined Vehicular Networking (SDVN) [14] [15] [16]. However, there are some open issues in the (SDN-Vehicular Network) coupling, especially about the SDVN vulnerabilities, and about the best way for implementing the controller to be suitable to the vehicular networks constraints, namely in centralized, decentralized or hybrid mode [4]. The routing and security features are implemented by the SDN Control Plane. Meanwhile, the data plane is devoid of intelligence, and acts only according to the controller rules. So, the location choice of the controller is critical, as the quality of service and the security depends on the robustness, the reliability and the availability of this controller.

In this paper, we present the impact of SDN architecture in vehicular network, and we propose to secure an existing SDN-based vehicular routing protocol by using a specific distributed trust model. In the proposed model, the vehicle's public keys are managed in a distributed way. Each new vehicle distributes

978-1-7281-1796-6/19/$31.00 ©2019 IEEE

its public keys to its neighbors. Besides, the described approach aims to assign a trust value to each vehicle. The trust is principally estimated by using the observations of historical interactions [17] inspired by the error log of HSDN-GRA routing protocol [6]. It measures the trust value of vehicles with respect to three types of unreliable behavior that a vehicle had in a period of time. The list of each vehicle's misbehavior is stored in an error log and embedded on a specific cluster head vehicle according to the description of HSDN-GRA routing protocol. The estimated trust value will determine if a vehicle will be chosen as next hop or not. As a positive result of the proposed scheme, three important security criteria are achieved: it aims to guarantee the authentication of vehicles and the integrity of the data by a signature mechanism, while the confidentiality of the exchanged data is ensured by an encrypted function. The goal is to protect a routing protocol based on SDN architecture against security threats and some attacks such as: replay attack, position faking, traffic analysis, message alteration, black hole attack, etc.

The present article is organized as follows: Section II describes the routing and security issues in IoV and provides an overview of related works that have proved the positive impact of SDN architecture on vehicular routing protocols and security enhancement. Section III describes a realistic use case where SDN is adopted for secure and robust routing data from a source to a destination in IoV services. Finally, Section IV concludes the paper and summarizes main future works.

II. Routing and security issues in IoV

Most of the applications dedicated to the intelligent transportation systems work on a collaborative way. They are mainly based on the exchanged information between the vehicles to offer useful services. Consequently, routing is a crucial part of IoV, because it defines how different entities effectively exchange messages. Besides, another important point is to preserve the integrity of these messages and the whole network. some mechanisms are used to ensure that data is exchanged in a secure manner.

A. SDN-based vehicular routing protocols

Routing in vehicular network is a big challenge because of high mobility leading to a very dynamic topology. In the traditional vehicular network architecture, position based routing strategy has been considered as the most promising approach [18] [19], it use Global Positioning System information and digital road maps. The geographic routing strategies are independent of the rapid changing topology. However, the investigation done in the paper [20] identifies some weaknesses, since traditional vehicular network architecture does not integrate intelligence and flexibility in routing protocols, as it is required by IoV entities, besides, the evolving context of IoV is not considered [15]. There are several contributions about SDN in vehicular networks routing protocols.

Sharifi et al. propose in [5] an Optimal Resource Utilization Routing scheme (ORUR) which balances the load of communication paths over the whole urban road segments, consequently, it prevents congestion of V2V communications while routing data on road segments, this is done by an SDN controller. Its main objective is to monitor real time connectivity and transmission delays on road segments. These values are translated to an optimization model called Weight Constrained Shortest Path Problem (WCSPP) and solved by an efficient algorithm to determine optimal routing paths among other existing routing paths which are already relaying data in the network. This approach incorporates load balancing and congestion prevention in the routing mechanism.

A multi-criteria routing protocol based on a hybrid SDN architecture is proposed by Alouache et al. in [6] The Hybrid SDN-based and Geographic Routing Protocol (HSDN-GRA) try to increase the communication reliability and availability while minimizing link breaks, reducing resolution costs and keeping a good end to end delay. HSDN-GRA uses periodic beacon messages. The proposed controller that makes decisions about where data is sent combine three different criteria: contact duration, free load metric embedded on each vehicle, and communication error logs which are handled by an elected node within clusters. Knowledge of inter-vehicle contact time permits a proactive avoidance and anticipation of premature link failures. The contact duration allows the selection of the next stable hop for data transmission respecting the load balancing. Finally, for more robustness, a dedicated log of error communication is hosted on a cluster head containing all error occurrences of the cluster members. Before choosing a relay, the error log is solicited to verify if the vehicle does not have a high frequency of errors. The presented simulation results show that HSDN-GRA achieves good performances.

In [21], Venkatramana et al. proposed a logically centralized but physically distributed SDN architecture to route packets in path with less congestion and link breakage, even in a dynamic and scalable network. Their routing protocol named SDN-enabled Connectivity-aware Geographical Routing Protocol (SCGRP) considers every vehicle as an open flow virtual switch consisting of a flow table. The SDN controller is on cloud. When the source vehicle receives the data packet from the input port, the flow table is looked upon to find if the destination IP address in the packet matches with the destination IP address existing in the flow entry. Then the vehicle will forward the data packet on the output port as specified in the flow table. If not, SCGRP selects the shortest path on digital map, as well as the junctions and sorts the road segments according to the desired density. The best relay with the smallest relative speed value is chosen. The process is repeated until the destination is achieved. If the access to the controller fails, another set of action is executed, the data packet is flooded to all the nodes within its vicinity and SCGRP is launched. When the forwarding vehicle goes down, the source vehicle notifies the controller of the failed action to re-handle the flow entries. The controller repeats the process and delivers an update message. The protocol is evaluated over the Centralized Routing Protocol [11] and proves its good

performances.

Ji et al. [10] describe an SDN-based geo-routing protocol (SDGR) for VANET, it combines an optimal forwarding path algorithm and a packet forwarding algorithm. Each routing client vehicle periodically transmits a state updating message to the routing server which updates the network state of vehicles. The routing client delivers directly the data packet to the destination if this one already exists in its routing table. Otherwise, it will send a request message to the routing server which executes the optimal forwarding path algorithm based on Dijkstra algorithm for calculating the packet's path to the destination. The optimal algorithm is adopted to find the shortest connected routing path with higher forwarding progress and vehicles density using network state vector and digital map. In addition, the optimal algorithm considers the vehicle density on each road to avoid sparse connectivity. After the optimal forwarding path is calculated, the routing server replies the routing client by sending a message that contains the optimal forwarding path, when the routing client receives the reply message, it will extract the path, and insert it into the new packet header which will be delivered to the next relay according to this path. Meanwhile, the packet forwarding algorithm is used to choose the ideal next-hop until the packet reaches the destination. The presented simulation results show that SDGR achieves good performances.

The SDN based routing protocols improve the communications which provide network access for both using unlimited computing resources on the internet, for storing, and uploading content to or from the internet, but in V2V communication mode, the network fragmentation, and the link failure can be caused by security issue.

B. SDN based security in IoV

The SDN architecture can also be a way to secure the network and to ensure the data integrity, thank to the SDN controller, a global overview of the system is achievable. To obtain network security, the controller collects information about the entire network traffic instead of exchanging a large amounts of information. As a result, it provides a better security mechanism than those applied to the traditional network [22].

1) Security attacks against vehicular networks: There are several attacks against security issue in vehicular networks. They are classified according to the security requirements they compromise [23]. Table I gives a non exhaustive list of vehicular networks attacks.

2) Security attacks against SDN architecture: The SDN architecture has also its own vulnerabilities, caused mainly by the location, the characteristics and the crucial role of the controller, and the exchanged flow between the control plane and the data plane [24].

Table II shows some attacks related to SDN architecture.

3) Security solutions for SDVN: Despite the vulnerabilities mentioned in Table I, SDN can be beneficial for the security issues in IoV, since it surpasses the limits of traditional mechanisms. Indeed, in IoV, the network is heterogeneous, and uses a set of technologies such as: WAVE, DSRC, LTE

TABLE I
VEHICULAR NETWORK ATTACKS VS SECURITY REQUIREMENTS

Attacks in vehicular networks	Authentication	Availability	Confidentiality	Integrity	Non-repudiation
Denial of Service (Dos)		x			
Distributed DoS		x			
Jamming		x		x	
Malware attack		x	x	x	
GPS Spoofing	x	x			
Hijacking of session	x				
Position faking	x				
Illusion attack	x	x			
Bogus information attack	x	x			
GPS Spoofing	x	x			
Snooping			x		
Identity reveling			x		
Location tracking			x		
Brute force	x		x		
Eavesdropping			x		
Sink Hole attack		x	x	x	
Black Hole attack		x		x	
Masquerade attack	x			x	
Message tempering				x	x
Message suppression				x	x
Message reply	x				x
Repudiation		x			x

TABLE II
SDN ATTACKS VS SECURITY REQUIREMENTS

SDN attacks in SDN architecture	Authentication	Availability	Confidentiality	Integrity	Non-repudiation
Dos on the Data plane		x			
Distributed Dos on the Control plane		x			
Controller identity spoofing	x	x	x	x	x
Flow based forwarding attack				x	x
Flow table alteration			x	x	

etc. with their own security policies, thus, due to the global view of the network, this huge set of security policies can be deployed without any conflict, which consolidates the security of the entire IoV system. Besides, the centralization and the abstraction given by the control plane allow administrators to update security policies using the incorrect behaviors observed as a support. When flows are identified as suspicious, the SDN allows to label them and isolate them by the controller, so, the data plane will not handle packets coming from these labeled flow. As a result, SDN improves security services in vehicular network. Table III describes some of them.

TABLE III
SECURITY IN IOV WITH SDN ARCHITECTURE

Action	details
Intrusion detection	The SDN controller represents an intrusion detection system as it monitors the whole network.
attackers identification	Monitor the control data flow to detect the modification in nodes settings.
Self recovery mechanism	After intrusion detection and attackers identification, the controller offers rules to automatic recovery against any attack.

C. Secure routing protocols based on SDN architecture

There is some recent research in literature which deals with both routing and security issues in vehicular networks using SDN architecture as a support.
Vasudes et al. propose the Improvised Trust based Ad-hoc On-demand Distance Vector routing (I-TAODV) [2] for secure routing in a multi hop scenario. I-TAODV is based on two algorithms, the first one identifies the trusted vehicles while the second the malicious ones, the two algorithms use a trust value calculation. Their protocol is based on SDN controller which monitors forwarding, reversing, trust of forwarding Vehicle, trust of reverse vehicle, path trust and network performances. in [25], Zhang et al. describe the Software-Defined Trust based Ad hoc On-demand Distance Vector routing (SD-TAODV) with trust management where the route discovery and the route maintenance process are moved into a controller, and the reverse and forwarding paths are chosen by the controller. The trust mechanism is a bi-objective function with two values: the node trust and the path trust computed respectively by Trust Node Calculation Process and Path Trust Calculation Process. These two metrics are needed to improve the Route Discovery Process of TAODV.

III. SECURING CONTROL PLANE FOR HSDN-GRA ROUTING PROTOCOL

The HSDN-GRA routing protocol described in the paper [6] uses an error log where three types of vehicle's misbehavior are stored: (Link failure, Random Beacon, and Non-Acknowledgement of previous message). The trust value of a vehicle is principally estimated by using an observation and a tracking of its previous interactions [17]. In this paper, we use the error log of HSDN-GRA routing protocol to measure the trust value of each vehicle, this trust dimension is added in order to secure the SDN based routing protocol described the paper [6]. The trust is described as the expectation and the belief that a vehicle has about other vehicles concerning future behaviors. Its estimation is based on 1) experiences and evidences collected in the past either direct or indirect, and on 2) the knowledge about the vehicles nature, and/or on recommendations from trusted entities [17] [26] [27].

In HSDN-GRA [6], routing rules are jointly governed by two types of controllers: the Cluster Head vehicle: which represents the semi-centralized controller, and the other vehicles within the cluster which represent the distributed controllers. The goal is to secure the southbound interface [15] between the semi-centralized controller in the Cluster Head and the other vehicles, as well as the V2V communication. The integrity and authenticity of the routing rules are crucial, as the robustness of the routing protocol depends on. Besides, the authentication and the confidentiality need to be reached.
Figure 1 describes a semi-centralized SDN architecture in

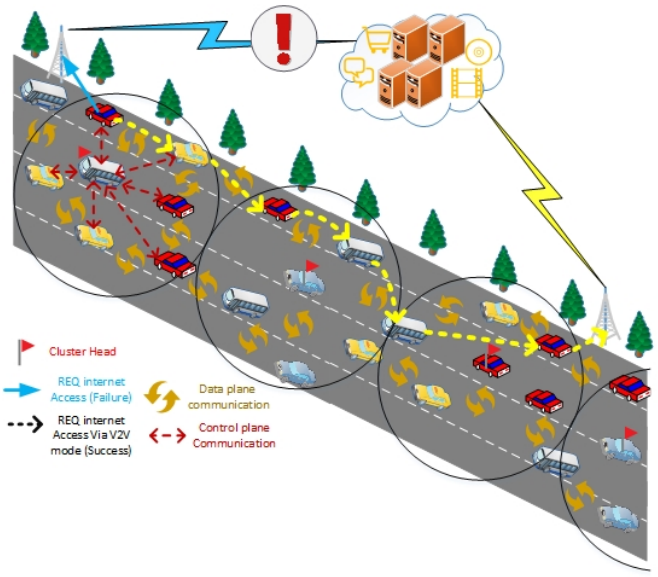

Fig. 1. Semi-Centralized SDN architecture in case of IoV communication

case of IoV communication scenario. This scenario uses the HSDN-GRA routing protocol. A vehicle tries to access to an internet service and fails, because it is inaccessible directly by the closest infrastructure. So it switches to the vehicles on the road for routing its request. The vehicles form clusters and a Cluster Head is elected. This cluster head contains a part of the control plane (the error log), the second part is distributed on the rest of cluster members. The internet access request transit through vehicles with a hop-by-hop strategy until reaching the destination. Each vehicle designates its next hop according to the control plane policy i.e : a balance between the vehicle communication capacity and its error frequency.

- Hypothesis:

-In this paper, the highway scenario is chosen, because of the stability of vehicle's speed.
Beacon message = $\langle id, x, y, v, \overrightarrow{dir}, l, isCH \rangle$. Where id is the identifier of the vehicle, x and y represent the geographical coordinates, v the speed of vehicle, $\overrightarrow{dir}$ the vehicle direction, l the free load of the vehicle in number of packets, and $isCH$ a boolean to specify if the vehicle is a cluster head or not.

-We briefly explain the HSDN-GRA protocol: it builds the routing path hop-by-hop, crossing gateways.
Some vehicles are in gateway status, because they are at the intersection of several clusters. Each vehicle sorts its neighbors in a list by decreasing value of packet reception capacity [6]. When a vehicle has packets to send, if there is a gateway among its direct neighbors, it will be chosen by default as best relay to pass through one cluster to another. If not the sender selects the head of its neighbors list, and asks the SDN controller embedded in the Cluster Head to check its trust and error frequency values in the log. If they satisfy the fixed conditions, the head of the list will be chosen as best relay, otherwise, the next element in the sorted list will be tested.

-At the beginning, the trust threshold and free load value of vehicles are set to equals and optimal.

-Malicious-Vehicles $\ll$Reliable-Vehicles.

The securing HSDN-GRA steps are :

- Step 0: Public key distribution

  -Each vehicle sends and receives a define Beacon [6] to and forms the one hop neighbors.
  -Each vehicle sends its Public Key $Pkey$ within neighboring, and receives back the $Pkey$ from each neighbor.
  -At this initialization step, there is only a distributed control plane embedded on each vehicle.

- Step 1 : Cluster Head election

  -After a period of time T, a distributed consensus occurs for the Cluster Head Election: the one with the largest free load and the high trust value, will be the Cluster Head.
  -The largest free load value is deducted from the receive Beacon.
  -The trust value of each vehicle is estimated and confirmed by the whole vehicles. -Initially, when there is no Cluster Head, logs are distributed within vehicles to monitor the communication errors of each neighbor. The defined trust rate is computed using the log of vehicle's misbehavior according to the formula 1:

$$Trust = (\frac{1}{ErrorOccurrences}) \quad (1)$$

  -Then, each vehicle broadcasts a list L of its neighbors, their associated $Pkey_i$ and their trust values:

$$L = \{(V_i, Pkey_i, Trust_i)\}, With\ i \in \{1,n\}$$

  -Finally, based on all the received lists L_i, a vehicle V confirms the reliable trust value of each neighbor V_i and the association $(V_i/Pkey_i)$.
  -The Cluster Head election, is done in a distributed manner. On each vehicle, the Cluster Head is the neighbor with the largest free load, and the highest trust value.
  -The variable "IsCh" will be $True$ in the Beacon for the Cluster Head, while the rest of vehicles will keep the value $False$.
  -The cluster Head represents the Semi-Centralized SDN controller used by HSDN-GRA where the log of communication errors is embedded.

- Step 2: Securing control plane of HSDN-GRA

  - The Secure HSDN-GRA is explained in this step.
  -After the Cluster Head election, all the Beacons are signed by the sender. The goal is to ensure the authentication. The structure of the Beacon message is shown by Figure 2.

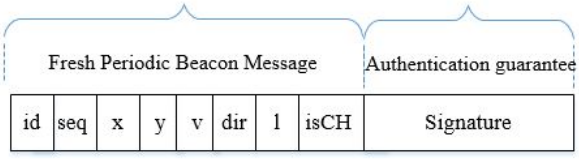

Fig. 2. Structure of Beacon Message in secure HSDN-GRA

we proceed to secure the southbound interface used in HSDN-GRA routing protocol [6].
The control decisions about the next hop are encrypted and signed by the semi-centralized controller in order to preserve the confidentiality and guarantee the authentication. Figure 3 shows the exchanged messages via the southbound interface.

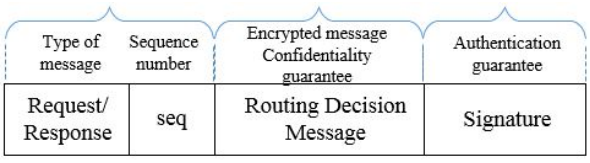

Fig. 3. Structure of southbound messages in secure HSDN-GRA

The identity of each vehicle is verified using a signature.In the southbound interface, the communications

are encrypted between the semi-centralized controller of the cluster head and SDN architecture of the cluster members. To do so, a symmetric encryption algorithm with AES [28] is adopted. Each vehicle shares with the Cluster Head a secret key K_s. This secret key is based on the public key already shared for signatures.To deduce K_s, a Vehicle and its corresponding Cluster Head exchange two random numbers $RAND1$ and $RAND2$ encrypted with the public keys. Every entity will extract the secret key using the formula 2.

$$Ks = (RAND1 \bigoplus RAND2) \quad (2)$$

Figure 4 shows a communication between the semi-centralized controller and other vehicles.

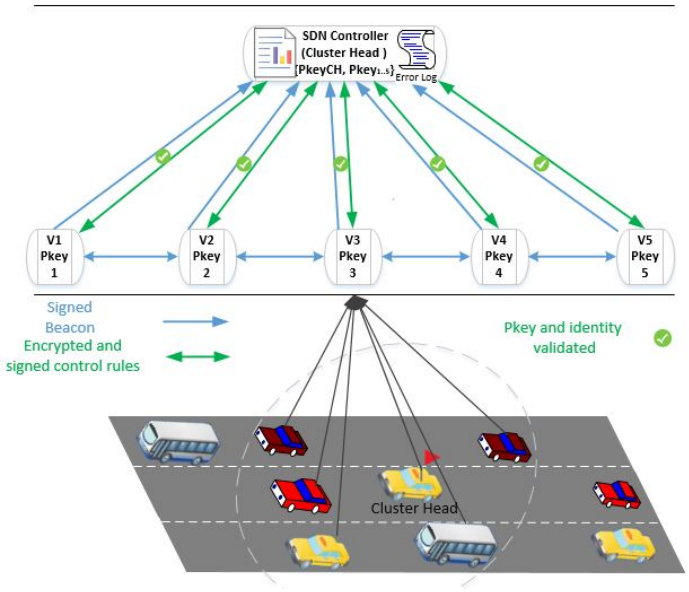

Fig. 4. Cluster vehicles Representation and Communication in secure HSDN-GRA

- Step 3 : Secure incoming vehicles in a cluster

  The integration of an incoming vehicle within a cluster is done on three steps:
  - The new vehicle V_n announce its self by broadcasting its Beacon and its Pkey.
  - The Cluster members reply to V_n with the identifier and the Pkey of the Cluster Head, while transfer the triplet (V_n,$Pkey_n$, $Trust_n$) to the Cluster Head.
  - The Cluster Head confirms the identity of V_n by analyzing the whole received triplets (V_n,$Pkey_n$,$Trust_n$) from the cluster members. It deduces the probability of the veracity of this triplet, from the number of vehicles who affirm it. Finally, it uses a Challenge-Response mechanism [29] to confirm that the new V_n has a private key corresponding to $Pkey_n$.

The step 3 is illustrated by Figure 5. It shows how an incoming vehicle in the Cluster is correctly integrated.

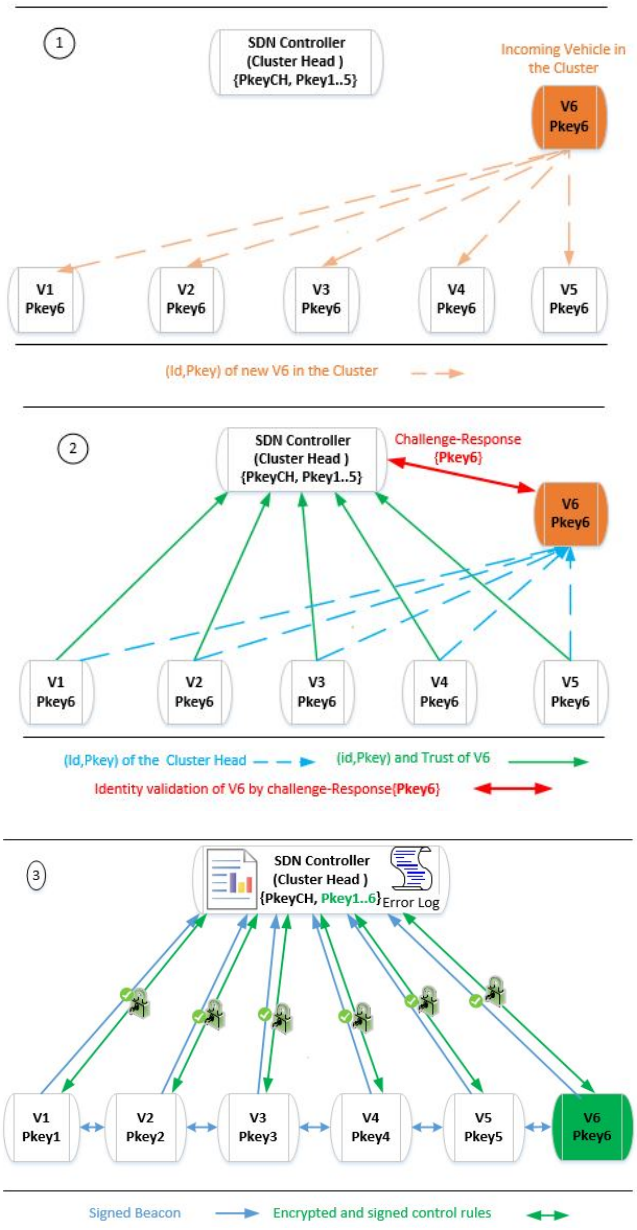

Fig. 5. New vehicle integration in the Cluster

- Step 4 : Secure outgoing vehicle from a cluster

  In this step, we describe how our approach detects and behaves, in a secure manner, when a vehicle leaves the coverage area of the cluster. We identify two cases:
  -The first case concerns a cluster member request of leaving the current cluster, for example, to join another cluster, the steps are:
  - The Cluster member sends a Request-to-Leave mes-

sage to the Cluster Head

- The Cluster Head uses a Challenge-Response mechanism [29] to ensure that the request comes from the pretending Cluster member.
- Once the authentication done, the Cluster Head sends an ACK message to this cluster member as an acknowledgement of Request-to-Leave message, then signs and broadcast a $Revoke(id, Pkey)$ message to the whole cluster members in order to revoke the key of the vehicle leaving.
- The cluster members reply with an ACK message confirming the revocation of this vehicle.

-The second case manages the leaving of the unstable and the unreliable cluster members, the ones that don't respect the periodicity of Beacons. In our approach, Beacons are supposed to be sent and received at every time-out τ. Besides, the Cluster Head assigns a Timer-of-Refresh ToF, initialized to 5τ, to each Cluster member sending a Beacon. ToF is launched and decremented by the Cluster Head, when a Cluster member Beacon is received.
If a Beacon is received from a Cluster member in the time interval [τ,5τ], so the ToF value is refreshed and reset to its initial value. Otherwise, the Cluster Head considers this Cluster member as unstable and decides to exclude it from the cluster. To do this, the procedure is similar to the case one:

- After ToF expired, the Cluster Head signs and broadcast a Revoke(id,Pkey) message to the whole cluster.
- The Cluster members send an ACK message confirming the revocation of this vehicle.

Figure 6 explains how our approach deals with a Cluster member outgoing scenario. It includes the two cases, as the scheme in the black circle describes the case in which the Cluster member asks for leaving, while the rest details the revocation procedure.

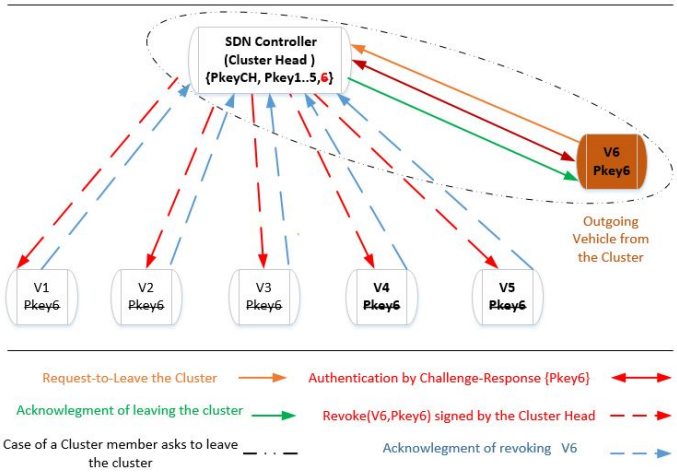

Fig. 6. Cluster member leaving management

IV. Conclusion

The SDN architecture has a positive impact on vehicular network. It facilitates the routing strategies by making optimal decision for routing while in traditional routing protocols data traffic sometimes becomes unbalanced because of the shortest routing path. It also selects the most suitable channels and frequencies for data transmission at a specific time according to the context and the requirements. Besides, it enhances security issues by allowing the implementation of adaptive security policies. In this paper, we have presented a secure HSDN-GRA for more robustness, by building a trust model between nodes, and securing the communication between the semi-centralized control plane and the SDN architecture of each vehicle. As future work, we will proceed complete and to improve the simulations for comparative values concerning the delay, packet delivery ratio, packet loss, and network overhead metrics.

References

[1] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa, and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[2] H. Vasudev and D. Das, "A trust based secure communication for Software Defined VANETs," in *2018 International Conference on Information Networking (ICOIN)*, Jan 2018, pp. 316–321.

[3] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular Ad-Hoc Networks: architectures, research issues, methodologies, challenges, and trends," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, pp. 1–11, 2015.

[4] A. Di Maio, M. R. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, and T. Engel, "Enabling SDN in VANETs: What is the impact on security?" *Sensors*, vol. 16, no. 12, 2016.

[5] M. Sharifi and A. Senhaji Hafid, "Routing in Heterogeneous Vehicular Networks using an adapted Software Defined Networking approach," in *The Fifth IEEE International Conference on Software Defined Systems (SDS-2018)*, Barcelona, Spain, 04 2018.

[6] L. Alouache, N. Nguyen, M. Aliouat, and R. Chelouah, "Toward a hybrid SDN architecture for V2V communication in IoV environment," in *The Fifth IEEE International Conference on Software Defined Systems (SDS-2018)*, Barcelona, Spain, 04 2018.

[7] R. M. Venkatesh, A Indra, "Routing protocol for Vehicular Ad-Hoc Networks (VANETs) : A review," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 1, 2014.

[8] B. Dong, W. Wu, Z. Yang, and J. Li, "Software Defined Networking Based On-Demand Routing Protocol in Vehicle Ad-Hoc Networks," in *2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, Hefei, Anhui, China, Dec 2016, pp. 207–213.

[9] R. Soua, E. Kalogeiton, G. Manzo, J. M. Duarte, M. R. Palattella, A. Di Maio, T. Braun, T. Engel, L. A. Villas, and G. A. Rizzo, "SDN coordination for CCN and FC content dissemination in VANETs," in *Ad-Hoc Networks*. Springer, 2017, pp. 221–233.

[10] X. Ji, H. Yu, G. Fan, and W. Fu, "SDGR: An SDN-Based Geographic Routing Protocol for VANET," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Dec 2016, pp. 276–281.

[11] M. Zhu, J. Cao, D. Pang, Z. He, and M. Xu, "SDN-based routing for efficient message propagation in VANET," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2015, pp. 788–797.

[12] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software Defined Networking-based Vehicular Ad-Hoc Network with Fog Computing," in *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*. IEEE, 2015, pp. 1202–1207.

[13] I. Ku, Y. Lu, M. Gerla, F. Ongaro, R. L. Gomes, and E. Cerqueira, "Towards Software-Defined VANET: Architecture and services," in *Ad-Hoc Networking Workshop (MED-HOC-NET), 2014 13th Annual Mediterranean*. IEEE, 2014, pp. 103–110.

[14] M. Chahal, S. Harit, K. K. Mishra, A. K. Sangaiah, and Z. Zheng, "A survey on Software-Defined Networking in Vehicular Ad-Hoc Networks: Challenges, applications and use cases," *Sustainable Cities and Society*, vol. 35, pp. 830 – 840, 2017.

[15] Z. He, J. Cao, and X. Liu, "SDVN: enabling rapid network innovation for heterogeneous vehicular communication," *IEEE Network*, vol. 30, no. 4, pp. 10–15, 2016.

[16] M. Kalinin, P. Zegzhda, D. Zegzhda, Y. Vasiliev, and V. Belenko, "Software Defined Security for Vehicular Ad-Hoc Networks," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2016, pp. 533–537.

[17] S. Soleymani, H. Abdullah, W. Hassan, M. H. Anisi, S. Goudarzi, M. Baee, and M. Satria, "Trust management in Vehicular Ad-Hoc Network: a systematic review," vol. 2015, 05 2015.

[18] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, "A survey on Position-based Routing for Vehicular Ad-Hoc Networks," *Telecommun. Syst.*, vol. 62, no. 1, pp. 15–30, May 2016.

[19] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of Vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[20] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of Vehicles: Architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–9, 2017.

[21] D. K. N. Venkatramana, S. B. Srikantaiah, and J. Moodabidri, "SC-GRP: SDN-enabled connectivity-aware geographical routing protocol of VANETs for urban environment," *IET Networks*, vol. 6, no. 5, pp. 102–111, 2017.

[22] P. Baskett, Y. Shang, W. Zeng, and B. Guttersohn, "SDNAN: Software-Defined Networking in Ad-Hoc Networks of Smartphones," in *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, USA, Jan 2013, pp. 861–862.

[23] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on Security Services in Vehicular Ad-Hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[24] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," *IEEE Security Privacy*, vol. 14, no. 4, pp. 34–44, July 2016.

[25] D. Zhang, F. R. Yu, Z. Wei, and A. Boukerche, "Software-Defined Vehicular Ad-Hoc Networks with Trust Management," in *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '16. New York, NY, USA: ACM, 2016, pp. 41–49.

[26] N. Bimeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in *2012 IEEE Vehicular Networking Conference (VNC)*, Nov 2012, pp. 78–85.

[27] J. Luo, X. Liu, and M. Fan, "A Trust model based on fuzzy recommendation for Mobile Ad-hoc Networks," *Computer Networks*, vol. 53, no. 14, pp. 2396 – 2407, 2009.

[28] J. Schaad, "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)," RFC 3565, Jul. 2003. [Online]. Available: https://rfc-editor.org/rfc/rfc3565.txt

[29] M. Rouse, "Challenge - response authentication definition: What does challenge - response authentication mean?" https://searchsecurity.techtarget.com/definition/challenge-response-system, accessed: 2018-05-30.