Security in vehicles with IoT by prioritization rules, vehicle certificates and trust management

Iván García-Magariño, Sandra Sendra, *Member, IEEE*, Raquel Lacuesta, *Senior Member, IEEE* , Jaime Lloret, *Senior Member, IEEE*

***Abstract*—The Internet of vehicles (IoV) provides new opportunities for the coordination of vehicles for enhancing safety and transportation performance. Vehicles can be coordinated for avoiding collisions by communicating their positions when near to each other, in which the information flow is indexed by their geographical positions or the ones in road maps. Vehicles can also be coordinated to ameliorate traffic jams by sharing their locations and destinations. Vehicles can apply optimization algorithms to reduce the overuse of certain streets without excessively enlarging the paths. In this way, traveling time can be reduced. However, IoV also brings security challenges, such as keeping safe from virtual hijacking. In particular, vehicles should detect and isolate the hijacked vehicles ignoring their communications. The current work presents a technique for enhancing security by applying certain prioritization rules, using digital certificates, and applying trust and reputation policies for detecting hijacked vehicles. We tested the proposed approach with a novel agent-based simulator about security in IoT for vehicle-to-vehicle (V2V) communications (ABS-SecIoTV2V). The experiments focused on the scenario of avoidance of collisions with hijacked vehicles misinforming other vehicles. The results showed that the current approach increased the average speed of vehicles with a 64.2% when these are giving way to other vehicles in a crossing by means of IoT.**

***Index Terms*—agent-based simulation, coordination, intelligent transportation, security, reputation, trust**

I. Introduction

Some smart vehicles can interact among each other, by means of Internet of Things (IoT), conforming a new field named as Social Internet of Vehicles (SIoV) [1]. Vehicles can cooperate for conforming Vehicular Ad hoc Networks (VANETs) with different routing protocols [2]. In addition, Internet of public transport vehicles can support VANETs by means of communication among vehicle groups that dynamically change [3]. In this context, vehicles can cooperate among each other (a) to avoid collisions, (b) to estimate the routes with least traffic, or (c) to arrange the best routes for avoiding waiting times in the charging stations for electric vehicles [4]. These are some of the most important issues that require the vehicles' data collection. These data should be transferred in a secure way with mechanisms like the existing one for big data collection from vehicles via a mutual authentication and single sign-on algorithm [5]. The security in the Internet of Vehicles (IoV) can also be useful for safely making the emergency rescue operations more efficient, and gathering reliable proofs of accidents such as the speeds and positions of vehicles [6].

Vehicles can connect among each other through vehicle-to-vehicle (V2V) communications and with the city infrastructure by means of vehicle-to-infrastructure (V2I) communications. Both kinds of communication can support real-time operations [7]. For instance, V2V communications can be useful for detecting traffic congestion in large-scale scenarios [8] or cooperating for car parking [9]. For example, V2I communications can support the stabilization of vehicle strings for reducing disturbances, with adaptive driving strategies [10]. In addition, vehicles can also use V2I communications in a street-aware and Intelligent Beaconless forwarding protocol for achieving fast and reliable communications in urban vehicular scenarios [11].

Vehicles with IoT and autonomous decisions on motion imply many challenges for the viewpoint of security and safety, as one can observe in the variety of possible attacks over self-driving vehicles [12]. If a vehicle is able to brake, turn or accelerate for avoiding a collision based on the information received by Internet, the car must completely validate the veracity of this information. Otherwise, a hijacked vehicle could provoke collisions or make other vehicles to unnecessarily stop. The hijacked vehicle would achieve this by intentionally sending wrong information to the other vehicles.

There are several mechanisms for performing traffic simulations. For example, model-driven development can be used for this kind of simulation as in the work [13], which defines a domain-specific modeling language for defining traffic simulations. In addition, agent-based simulators (ABSs) have proven to be useful for simulating IoV. In this context, vehicles are modelled as agents, and V2V communications are simulated as social interactions among agents [9]. In this line, agent technology was proposed to improve the routing in VANETs with a novel clustering algorithm [14].

Several works proposed different solutions for supporting authentication in vehicular networks. For instance, VANETs used authentication by means of the Elliptic Curve Digital Signature Algorithm in broadcast messages, considering privacy, probabilistic and defense from DDoS attacks [15]. In addition, Scheme for IEEE 802.11p was improved for

I. García-Magariño is with Department of Computer Science and Engineering of Systems, University of Zaragoza, Teruel 44003 and Instituto de Investigación Sanitaria Aragón, Zaragoza 50009, Spain, e-mail: ivangmg@unizar.es

S. Sendra is with Departamento de Teoría de la Señal, Telemática y Comunicaciones (TSTC), Universidad de Granada. Calle Periodista Daniel Saucedo Aranda, s/n, 18071 Granada, Spain. email: ssendra@ugr.es

R. Lacuesta is with Department of Computer Science and Engineering of Systems, University of Zaragoza, Teruel 44003 and Instituto de Investigación Sanitaria Aragón, Zaragoza 50009, Spain, e-mail: lacuesta@unizar.es

J. Lloret is with Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politècnica de València, Carretera Nazaret-Oliva, s/n 46730 Grao de Gandia, Valencia, Spain. email: jlloret@dcom.upv.es

Manuscript received April 19, 2005; revised August 26, 2015.

V2I communications with a lightweight authentication that focused on security and privacy of vehicles [16]. The trust management has proven to be useful in VANETs for maintaining security in VANETs considering probabilistic approaches, deterministic ones and combination of these [17]. Vehicles need to verify that the locations reported by other vehicles are both accurate and reliable. For example, R. Kasana et al. [18] improved the accuracy of locations by considering neighbor locations. In addition, S. Dalya Khalid et al. [19] used transferable belief models for ensuring security in the sharing of vehicle locations. When vehicular networks are open to other heterogeneous communications, these usually raise many security challenges, as reviewed by Kaiwartya et al. [20] when presenting their architecture for IoV. Some of these challenges are related with the location accuracy, location verification, location privacy and the operational management of all the traffic of the different networks.

In this context, the current work proposes an approach aimed at maintaining security and safety in vehicles with IoT. It combines proper authentication by asymmetric encryption, prioritization rules and management of trust and reputation over vehicles identifiers. The current approach is illustrated with a novel ABS about security in IoT with V2V communications (ABS-SecIoTV2V).

The current article is organized as follows. The next section introduces the most relevant related work highlighting the gap covered by the current work. Section III presents the technique for achieving security in the IoV from virtual hijacking focusing on respectively the prioritization rules, the vehicle certificates and the trust management. It also presents the novel ABS about collision avoidance in crossroads for illustrating the current approach. Section IV presents the experiments that we conducted for assessing the current approach. Finally, section V mentions the conclusions and depicts some future research lines.

II. Related work

This section presents some relevant works related to collaborative autonomous vehicles, IoT supported vehicles and the infrastructure needed to support this.

The development of infrastructures that offer support for smart vehicle networks, nowadays, due to the evolution of smart cities is one of the most relevant topics of the decade, conforming fields such as IoV. This type of infrastructure will try to maximize communications for allowing the safe transit of autonomous vehicles [21]. This application has implicit important aspects to deal with, such as road safety and the correct prioritization of traffic, according to a series of rules. The final goal of developing this kind of infrastructures could be reaching destination on time.

One of the most important issues to take into account is how to predict the traffic density and estimating the required time to reach a destination [22]. In this sense, R. Sun et al. [23] proposed a cooperative vehicle infrastructure system to control and monitoring the traffic speed and density using microscopic data. Their model was based on the hypothesis that a vehicle will move to the downstream during a period of time. Therefore, the travel distance of each vehicle was calculated using its average speed during a single time step, and its speed was influenced by several consecutive links instead of one. For predicting the speed of a vehicle, they considered the evolution of the average speed of the different downstream links and the current link. Finally, by registering the number of vehicles in each link, it was possible to calculate the traffic density. Therefore, combining the traffic density of the link and the average speed of the vehicle, it was possible to determine the macroscopic variables during the established time period. The results showed that through the proposed model it was possible to foresee the congestion points.

Another relevant approach was presented by R. Kala [24]. This work presented an intelligent transportation system to decrease the travel time of vehicles and avoiding congestions. The article aimed at making the transportation system cooperative to favor the vehicles for not running late. The author modelled the mechanism by which a vehicle judged its running status and decided whether to ask for cooperation. The mechanism was able to combine and coordinate the vehicles movement, the traffic lights and lane changes, which helped to prioritize the vehicles running late. Experimental results showed that a lesser number of vehicles reached their destinations late when using their approach.

Several works proposed trust management mechanisms for vehicles with IoT. For instance, A. Bhargava et al. [25] proposed a trust scheme to improve the vehicle's safety and security in IoV. The proposal was based on the Dempster Shafer Theorem (DST) to imbibe uncertainty and lack of sufficient data about a vehicle for quick trust update. Authors used the iterative trust computation based on the direct interaction with the vehicles and feedback from the neighbors. The model took into account four different trust levels for characterizing vehicle's behavior. Results showed that the mechanism could be scalable and was suitable to be used in IoV environment even when vehicle exhibited changing behavior in presence of a small number of vehicles in the neighborhood. Moreover, F. Gai et al. [26] proposed a Ratee-based Trust Management (RTM) system that guaranteed that each node stored its own reputation information recorded during the past transactions. Authors also introduced a credible CA server to be sure the integrality and the non-deniability of the trust information is guaranteed. The RTM was implemented taking SIoV into account where the relationships established between nodes were utilized to enhance the accuracy of trustworthiness. In their experiments, their proposed scheme presented faster convergence and higher transaction success rate, and the time cost for calculating trustworthiness met the demand of vehicular networks.

Wu He et al. [27] presented an interesting modular multi-layered vehicular data platform based on cloud computing and IoT technologies. Along the paper, authors discussed on the cloud services and how they could be implemented to perform and make intelligent decision for the correct vehicular data management. Authors proposed a novel software architecture for the vehicular data clouds which presented the capabilities of integrating several IoT devices available in vehicles and in the road infrastructure.

Furthermore, it is important to highlight that a smart and secure vehicular network should incorporate the use of sensors. In this sense, A. Mansoori and C. Acha [28] proposed the use of intelligent wireless sensor networks to prevent loss of electricity by the unnecessary usage of street lights at night. The system was based on the use of ultrasonic sensors, RASPBERRY PI3 and camera module installed on road to detect the vehicles that were not following the traffic rules.

Some ABSs simulate traffic, since agents can adopt different drivers' behaviors in vehicles as well as other people such as pedestrian. For instance, E. Karaaslan et al. [29] presented an ABS for simulating the repercussion of electric vehicles on the safety of pedestrians because these vehicles have silent engines. Their simulated results showed that the pedestrian traffic safety risk increased 30% with electric vehicles under high ambient sound levels, and it increased 10% under low sound levels. In addition, K. Malecki [30] developed an ABS about the influence of drivers' behaviors when looking for on-street parking on the traffic flow. Their simulated results showed that efficient on-street parking of motorists and car drivers paying attention to streamlined parking improved traffic flow efficiency significantly. However, none of these ABSs simulated strategies for maintaining security on vehicles with IoT when there were hijacked vehicles.

Nevertheless, none of the aforementioned works combined prioritization rules, digital vehicle certificates with asymmetric encryption and trust and reputation policies, in order to make vehicles secure from misinformation of hijacked vehicles. The current work covers this gap of the literature with the technique proposed in the next section.

III. Technique for maintaining security in vehicles with IoT

The current work proposes to maintain security in vehicles with IoT by combining prioritization rules, vehicle certificates and trust management. Figure 1 shows an overview of the current approach. Each vehicle with IoT includes the installation of the mechanism for taking decisions based on the prioritization rules in order to determine which orders should follow. Each vehicle has a validated certificate represented by a private key of asymmetric encryption provided by an official certifier entity. The vehicles can interchange signed messages and authenticate the identity of the sender by using the public key provided by the official certifier entity. The vehicles can manage the trust on vehicles by analyzing whether theirs messages have any misinformation. Vehicles also share the direct trust in a peer-to-peer distribution model, so vehicles can take decisions based on the reputation of the vehicle that is sending the messages.

The subsections describe each of the most relevant aspects of the current approach. Subsection III-A describes the prioritization rules that are involved in the decision-making process of vehicles. Subsection III-B indicates the certification mechanism used by vehicles. Subsection III-C introduces the trust and reputation mechanism of the current approach. Subsection III-D presents the ABS for illustrating and assessing the current approach.

A. Prioritization rules

Self-driving vehicles can have an interface for communications and coordination among vehicle. This approach proposes to add a layer just right after the kernel of the operative system of the vehicle with some prioritization rules for basic security. This layer should not have writing permissions for any user. In this way, no one would be able to overwrite it.

In this safe layer, the vehicle will not able to accelerate if another vehicle is closer than a proximity threshold based on the proximity sensor. The car will not turn right if this means going out of the road or crashing to any object. In this way, the vehicle will avoid collisions that can be avoided by their own sensors. This layer constitutes the first level of priority.

In the second level of priority, the orders of the driver are followed unless breaking any of the very basic rules of the aforementioned first level.

In the third level of priority, vehicles can take actions based on IoT. This could support self-driving supervised by the driver. This is the level that needs the security measures for avoiding collisions or any damages due to misinformation by hijacked vehicles.

This current approach authenticates vehicles by digital certificates, and manages trust and reputation to decide whether to rely on the information provided by a vehicle. Figure 2 shows the block diagram regarding the application of the prioritization rules when receiving an order or information from another vehicle with IoT. The first step is to apply the asymmetric encryption to determine whether the sender is authenticated. If the sender is not authenticated, then the message is completely ignored because (a) it is not reliable, (b) neither can trust and reputation be built about an unidentified sender. Then, the current approach applies the three aforementioned security layers based on the prioritization. Finally, the current approach analyzes whether the information provided by the sender was reliable. In this way, the current vehicle can update its trust on the sender and share this trust with peers.

B. Vehicle certificates

The current technique relies on the authentication of vehicles. In particular, each vehicle should have an identifier based in the number of the license plate. This approach uses asymmetric encryption for this purpose. This technique proposes to apply the Digital Signature Algorithm (DSA) for the asymmetric encryption as it is well-validated that it is secure for signing messages, and it is commonly used by public institutions. The owner or manufacturer of each vehicle requests a digital certificate through the online service provided by the certifier. Then, they bring the vehicle to the certified accreditation center. This makes sure that this vehicle is the one identified by its number with a double check with the manufacturer of the vehicle. Then, the certified accreditation entity provides a private key to the vehicle, so this can incorporate in their system without reading permission, so no one can access it. The certified accreditation entity makes its public key available, so that other vehicles can verify the identity of this vehicle.

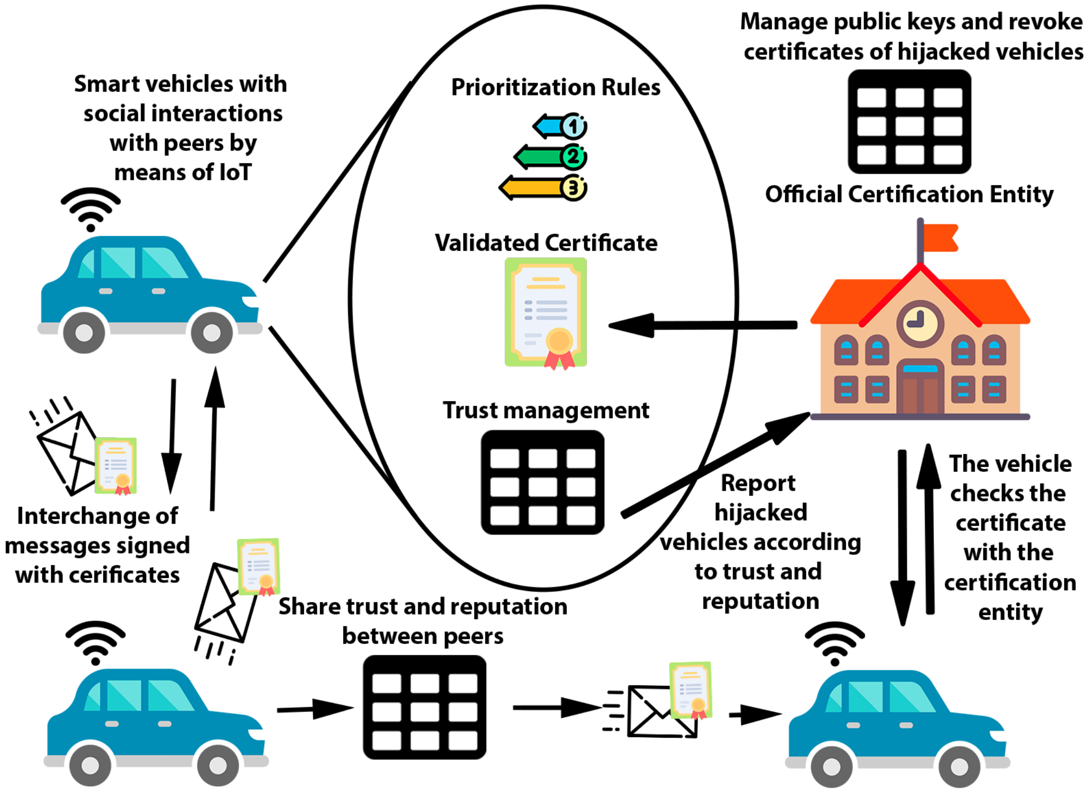

Smart vehicles with social interactions with peers by means of IoT
Prioritization Rules
1
2
3
Validated Certificate
Trust management
Manage public keys and revoke certificates of hijacked vehicles
Official Certification Entity
Interchange of messages signed with cerificates
Report hijacked vehicles according to trust and reputation
The vehicle checks the certificate with the certification entity
Share trust and reputation between peers

Fig. 1. Overview of the proposed technique for maintaining security in vehicles with IoT

From this point forward, the vehicle will sign all its messages with its validated certificate. The other vehicles can verify its authenticity by decrypting the hash summary of the message with the public key provided by the certified identity.

In order to maintain the security, vehicles will only consider messages authenticated with this system. In this way, even hijacked vehicles will need to sign their messages with their true identifier for communicating with other vehicles. Even though, hijacked vehicles could send misinformation with their true identity. In order to avoid the impact of these attacks, the current approach uses the trust and reputation policy introduced in the next section.

C. Trust and reputation management

The current approach uses trust and reputation management for tracking the vehicles with malware in order to isolate these and discard their messages.

For this purpose, vehicles corroborate the information received by other vehicles with the information sensed by their own sensors in real-time and afterwards. In some cases, a vehicle could ask other vehicles about the information sensed with their sensors in order to further analyze some cases of possible misinformation.

For example, if a vehicle X reports a location and a speed that will imply a collision on a vehicle Y in a crossroads and asks it to stop, then vehicle Y is forced to stop to give way to vehicle X. However, vehicle Y will check if any vehicle gets to the crossroads with its sensors. If that is not the case, vehicle Y assumes that vehicle X reported an unnecessary alert message, and classifies this message as suspicious. In some unlikely cases, it could have happened that vehicle X needed to stop for any other reason. Thus, it cannot be directly classified as malicious but if these suspicious messages are frequent by one vehicle, then this approach assumes that it has a malicious behavior. In each vehicle, the trust model is constituted by recording the number of messages received by each other vehicle and the number of these that were classified as suspicious. Each vehicle trusts another vehicle if either it has not enough data about it or the ratio of non-suspicious messages divided by the number of interchanged messages surpasses certain threshold. This approach does not only consider the trust based on direct contact with a vehicle, but also the reputation which is this same information observed by other vehicles. This information can be shared by both V2V communications or through a common databased managed by a certified institution. In this shared model, the reputation is also evaluated by calculating the ratio of non-suspicious messages divided by the number of interchanged messages and comparing this ratio with a threshold.

In this way, each vehicle can have a direct trust on another vehicle regarding the direct messages interchanged with it. The vehicle can also have information trust of other third-party vehicles on another vehicle, which is normally referred as reputation in the specialized literature [31]. The reputation is propagated through V2V communications, in which the trust of vehicle X on vehicle Y is propagated signed with

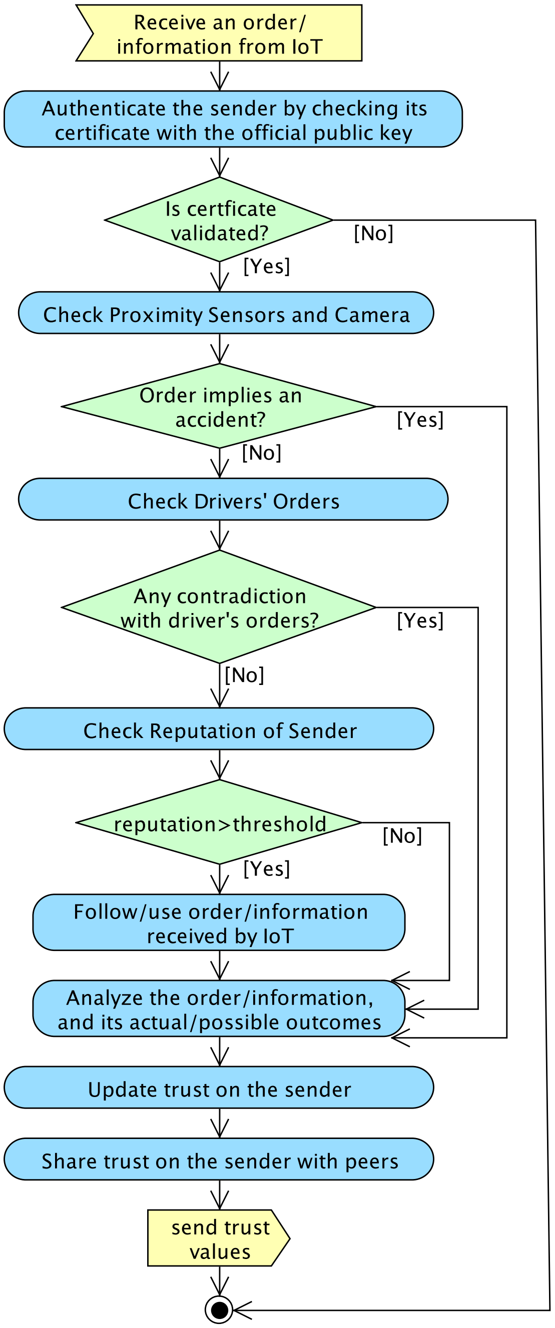

Receive an order/ information from IoT
Authenticate the sender by checking its certificate with the official public key
Is certficate validated?
[No]
[Yes]
Check Proximity Sensors and Camera
Order implies an accident?
[Yes]
[No]
Check Drivers' Orders
Any contradiction with driver's orders?
[Yes]
[No]
Check Reputation of Sender
reputation>threshold
[No]
[Yes]
Follow/use order/information received by IoT
Analyze the order/information, and its actual/possible outcomes
Update trust on the sender
Share trust on the sender with peers
send trust values

Fig. 2. Block diagram regarding the prioritization rules

a validated certificate by vehicle X. In this way, hijacked vehicles cannot significantly alter the reputation of any vehicle, since it cannot send trust scores with false identifiers. In addition to the fast and peer-to-peer communication in real-time through the network, vehicles will report this information also to the certification entity. This entity will collect this information, and if the reputation of vehicle is below certain threshold with a representative amount of data, then the entity revokes its certificate, until the software of this vehicle is reset to its initial state by the manufacturer.

By means of this approach, the hijacked vehicles will be discarded, and all its communication will be ignored by other vehicles, when the certification entity has detected its misbehavior. The manufacturer can revise the vehicle and ask again for a validate certificate with the commitment of investigating the reasons why this vehicle was hijacked.

D. Agent-based simulator for testing security strategies

This work includes the novel ABS called ABS-SecIoTV2V for defining and assessing different variations of the strategies applied in the current technique. This ABS has been developed following TABSAOND (a technique for developing ABS apps and online tools with nondeterministic decisions) [32] in order to simulate non-deterministic decisions in realistic scenarios. This ABS has developed with NetLogo simulation tool, since this tool has proven its utility for simulating different kinds of networks [33]. In the initial stages, we also considered using a specific environment for traffic simulation instead of NetLogo, and more concretely the most feasible option was the open-source RoadTrafficSimulation environment. However, we finally selected NetLogo because it explicitly used and agent-based approach with common operations such as explicit and implicit communications among agents, which were useful for designing V2V communications and managing the information received from vehicle sensors about other vehicles. In addition, NetLogo was designed for allowing users to easily define different agent behaviors, being this useful not only for implementing different security agent strategies but also implementing different behaviors of hijacked vehicles. Although RoadTrafficSimulation was open source and theoretically could be modified in anyway, the implementation of these agent strategies would have required firstly to implement some basic operations and to refactor some of its underlying structure. We selected NetLogo to avoid all this extra initial development effort and time.

In this ABS, the vehicles of the horizontal road give way to the vehicles in the vertical road. The horizontal vehicles ask the positions of vertical cars to them through IoT in order give them way when approaching the crossroads. One of the vertical cars simulates to be hijacked and reports fake positions. In particular, it provides the position of the crossing, so the vehicle waits in the give-way even if it is not necessary. In other words, the hijacked vehicle performs an attack in which another vehicle activates the brakes unnecessarily as it is informed about the existence of a fake possible collision. The hijacked vehicle only provides fake positions to vehicles in a limited distance range, so its behavior is more difficult to be detected.

Figure 3 shows the main excerpt of the User Interface (UI), which includes the input controls and the graphical visualization of the simulation. In the vertical cars, the hijacked car is represented with red, while the others are represented with blue. The horizontal cars use random colors. As commonly in NetLogo simulators, the “Setup” button reset the simulator to its initial state, and the “Go” button runs and pause the simulation alternatively. The simulator also allows users to select the number of cars visible in the simulation in respectively the horizontal and vertical roads. Notice that ABS-SecIoTV2V uses a wrapped map in which when a vehicle agent leaves the screen, it enters again in the opposite side, and consequently a few number of agents can simulate a continuous traffic of vehicles.

Figure 4 shows the UI graph about the speed of the vehicles that give way in the crossing. It represents the average speed of all the vehicles in each simulated second (denoted as "Speed" in the graph or also instantaneous speed in this article). This graph also shows an average speed from the beginning of the simulation to the current moment (referred as "Avg. Speed" in the graph). It is worth noting that the instantaneous speed has large variations since it is very sensible to the number of vehicles stopped in the crossing for giving way to any vehicle.

IV. Experimentation

In this experimentation, we used six vehicles in the horizontal road and three vehicles in the vertical road simultaneously displayed in the visualization of the simulation in ABS-SecIoTV2V. The horizontal vehicles give way to the ones in the vertical road.

In order to assess the current approach, we simulated ABS-SecIoTV2V with the currently proposed security approach and with a control mechanism. Both used the same behavior related with traffic, in the sense that in both mechanisms the horizontal vehicles gave way to the other vehicles in the crossing considering the same threshold distance and the same area for stopping. In both scenarios, vehicles reached 50 Km/h when they did not have to give way to other vehicles.

The difference between the current approach and the control one is that the latter one relied on the information provided by other vehicles, while the current one followed all the steps mentioned in section III.

Figure 5 shows the results of speed when using the current approach. This graph shows the instantaneous average speed of all the vehicles in the road with the give-way in every second, and is referred as "Speed". The speed had large variations, because in the crossroads some vehicles had to stop to give way to other vehicles, and consequently these stopped vehicles had a speed of zero value. The number of stopped vehicles varied regarding the coincidences of vehicles in the crossroads from different directions. It also shows the average speed considering these same cars but from the beginning of the simulation referred as "Avg. Speed". One can observe that the final global average speed was 37.1 Km/h of the vehicles in the road with the give-way.

Figure 6 shows the simulation results when using the control mechanism. In this scenario, the vehicles were not prepared to detect fake V2V communications, and consequently they did not detect the misinformation from the hijacked vehicle. As one can observe in the speed of cars, higher amounts of cars stopped more frequently as they used the brakes to give way in cases that was not necessary. The final global average speed was 22.6 Km/h.

Figure 7 compares the average speed between the current approach and the control one. From the instant of 150 s of simulation until the end (i.e. 1000 s of simulated time), the average speed of the current approach was considerably higher than with the control mechanism. The current approach had an improvement percentage of 64.2% in the final global average speed of vehicles. The average speed improved because with the current approach vehicles were able to detect the misinformation of hijacked vehicles, by means of the trust and reputation mechanism. In this manner, hijacked vehicles were not able to force other vehicles to stop unnecessarily by taking advantage of their vulnerabilities of the collision-avoidance safety system. It is worth mentioning that when the simulation had dense traffic, if a vehicle was unnecessarily forced to activate their brakes in a crossroads for a while, then all the other vehicles following this vehicle also needed to stop forming a queue of vehicles waiting to the first one to cross the crossroads. Thus, avoiding all these circumstances with the current approach improved the traffic flow performance as reflected in the increase of average speed of vehicles.

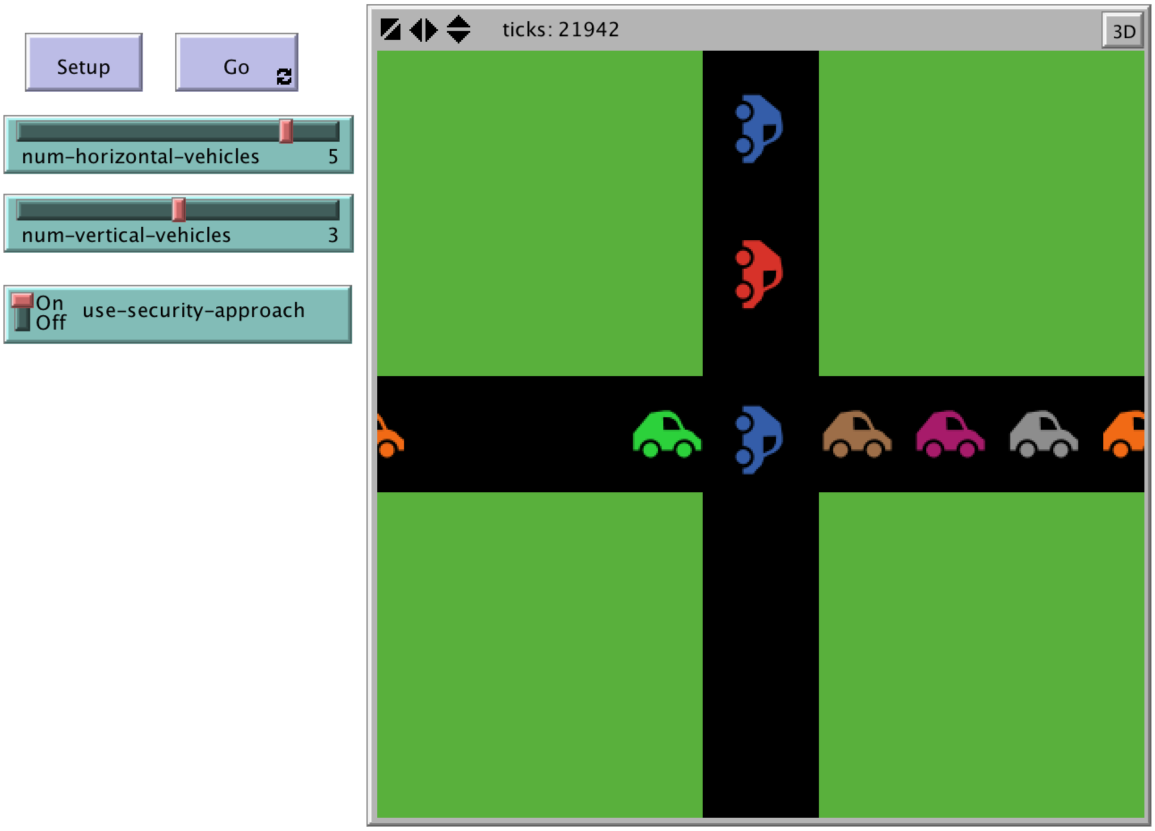
Moreover, we tested the trust and reputation mechanism. In this case, we used a different ABS that allowed us to simulate a larger number of vehicles. This ABS was inspired by the existing ABS-TrustSDN [34], with the differences of having peer-to-peer distribution of reputation and revocation of certificates by the official certifier.

In particular, we simulated that 95% of the messages with non-compromised vehicles were considered as reliable. We did not consider that all the messages were properly detected reliable since traffic depended on many variables including the different calibration of sensors (e.g. proximity, cameras and so) and environmental circumstances.

We simulated hijacked vehicles with smart strategies in which only 30% of the messages where intentionally malicious. Thus, other vehicles classified 65% of the messages of hijacked vehicles as reliable. In this way, hijacked vehicles were more difficult to be detected. In this simulation, we used 85 normal smart vehicles with IoT and 15 hijacked vehicles.

In this approach, we used a reputation strategy based on the history of failures of each vehicle for determining the trust on each vehicle. This strategy was based on post-analyzing the communications with a specific vehicle to determine whether the messages from these vehicles were suspicious (probably sending false information). This method required a minimum number of post-analyzed messages (i.e., 5) for calculating a representative trust assessment on this vehicle. After this minimum window threshold was reached, this vehicle was trusted only if the ratio of non-suspicious messages in the recorded history were equal or greater to a certain threshold (i.e., 60%). This assessment was performed by all the available information propagated among the different vehicles conforming the reputation of the vehicle.

Figure 8 compares the evolution of the average reputation of smart vehicles with IoT and the reputation of hijacked vehicles. The reputation was recalculated in each interaction among vehicles with IoT, and consequently the graphs shows the evolution along the number of interactions, which is displayed in the abscissa axis. The average reputation is represented as a percentage, in which 100% represents the highest reliability according to the collected trust measurements reported by peers. As one can observe, the reputation of hijacked vehicles dropped down in comparison with other



ticks: 21942

num-horizontal-vehicles 5

num-vertical-vehicles 3

On Off use-security-approach

Fig. 3. Input controls and graphic simulation in the UI of ABS-SecIoTV2V

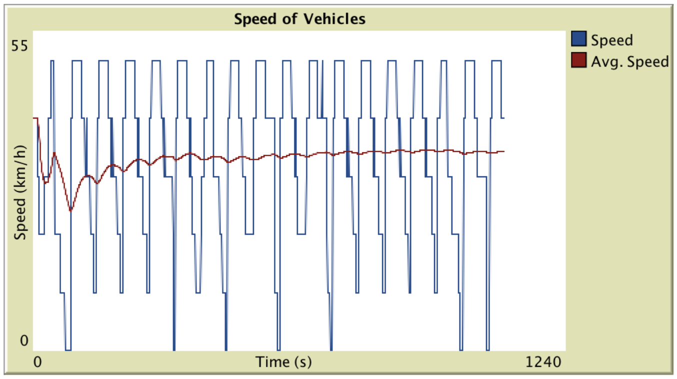


Fig. 4. Graph about speed in the UI of ABS-SecIoTV2V

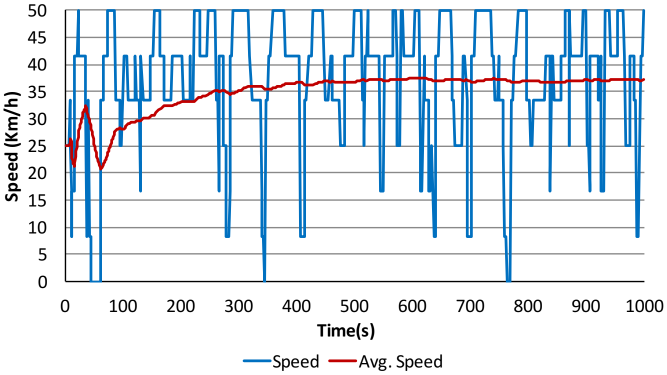


Fig. 5. Speed of vehicles with the current technique

vehicles, whose reputation increased to values near 100% over the time. Thus, vehicles properly detected the hijacked vehicles and reported these to the certifier entity. In this way, their certificates were revoked and the other vehicles ignored their messages. It is worth mentioning that the reputation of hijacked vehicles did not drop to almost zero, because once the certification entity revoked their digital certificates, their messages were no longer analyzed and their reputation was not updated anymore.

V. Conclusion

This article has proposed a technique for maintaining security in vehicles connected to Internet from virtual hijacking. This technique combines the use of prioritization rules from discarding some virtual attacks by relying more on sensors and drivers' actions. It uses digital certificates with a certification entity and asymmetric encryption in order to authenticate the messages from the real vehicles and keep track of their messages and actions. This technique uses peer-to-peer trust and reputation policies to isolate the hijacked vehicles and ignore their messages. The novel ABS-SecIoTV2V simulator applies this technique for the scenario of automatically avoiding

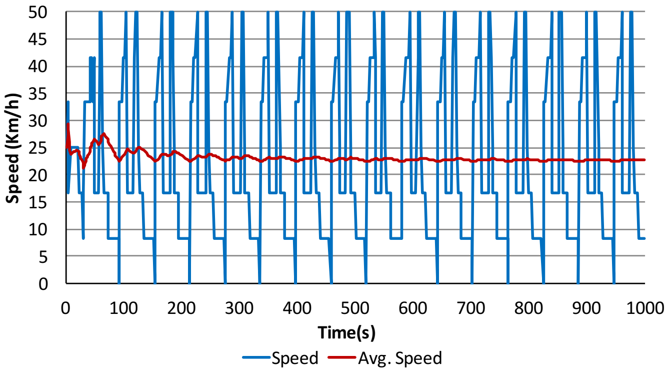


Fig. 6. Speed of vehicles with the control mechanism

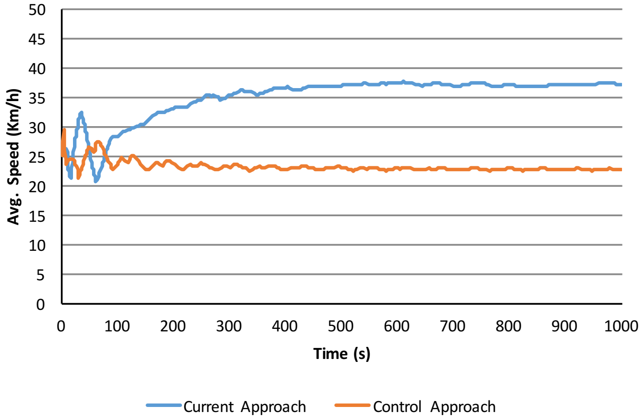


Fig. 7. Comparison of average speeds of vehicles between the current technique and the control mechanism

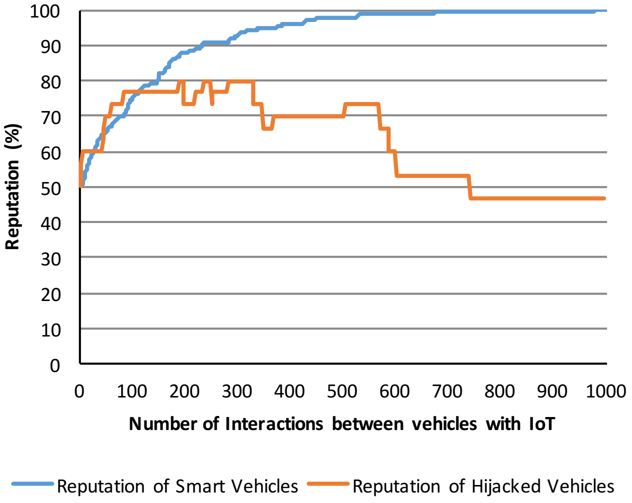


Fig. 8. Comparison of reputation between normal smart vehicles and hijacked ones with the proposed technique

collisions with IoT by activating the brakes when a collision is forecasted in a crossroads. The hijacked vehicles report their fake locations so other vehicles unnecessarily activate their brakes when there is not any danger of collision. The simulation results showed that in the current approach vehicles properly distinguished between hijacked vehicles from others, by managing trust and reputation based on the information directly observed and the one received from other vehicles. The simulation results also showed that the current approach improved the traffic flow performance as reflected in the increase of average speed of vehicles.

The current work is planned to be extended by applying the current approach in other virtual attacks on vehicles connected to Internet. For example, we will apply the current approach for avoiding misinformation regarding fake locations to make confusion in the coordination for avoiding traffic jams. Another future work is to assess the current technique when executed with common vehicle processors and communications to measure the response times of both the algorithms and the involved communications, in order to determine if this approach is feasible for avoiding accidents in real-time. In order to commercialize the current approach, we will need to work separately in three different components. First, we will need to develop a component that supports V2V communications through the most accepted regulation in the European Commission, which is probably ITS-G5. This component needs to be integrated within the vehicle and we will implement it in collaboration with some vehicle manufacturer. The second module will provide a high-level programming interface to access all the operations of the vehicle, and again we will need the collaboration with the vehicle manufacturer. The third component will translate the proposed strategies to the corresponding programming language with access to the two other components. Finally, we would need a great private or public investment for marketing and promoting the use of vehicles with this extra functionality of secure coordination among vehicles. In this process, we will try to provide a low-cost solution so it can become popular and feasible from a business-model viewpoint.

Acknowledgment

This work acknowledges the research project “Construcción de un framework para agilizar el desarrollo de aplicaciones móviles en el ámbito de la salud” funded by University of Zaragoza and Foundation Ibercaja with grant reference JIUZ-2017-TEC-03. We also acknowledge support from “Universidad de Zaragoza”, “Fundación Bancaria Ibercaja” and “Fundación CAI” in the “Programa Ibercaja-CAI de Estancias de Investigación” with reference IT1/18.

References

[1] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, “Social internet of vehicles: Architecture and enabling technologies,” *Computers & Electrical Engineering*, vol. 69, pp. 68–84, 2018.

[2] K. Z. Ghafoor, M. A. Mohammed, J. Lloret, K. A. Bakar, and Z. M. Zainuddin, “Routing protocols in vehicular ad hoc networks: survey and research challenges,” *Network Protocols and Algorithms*, vol. 5, no. 4, pp. 39–83, 2013.

[3] J. Lloret, A. Canovas, A. Catalá, and M. Garcia, “Group-based protocol and mobility model for VANETs to offer internet access,” *Journal of Network and Computer Applications*, vol. 36, no. 3, pp. 1027–1038, 2013.

[4] I. García-Magariño, G. Palacios-Navarro, R. Lacuesta, and J. Lloret, "ABSCEV: An agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles," *Computer Networks*, vol. 138, pp. 119–135, 2018.

[5] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale Internet of vehicle," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 601–610, 2017.

[6] H.-T. Wu and G.-J. Horng, "Establishing an Intelligent Transportation System With a Network Security Mechanism in an Internet of Vehicle Environment," *IEEE Access*, vol. 5, pp. 19 239–19 247, 2017.

[7] N. Torabi and B. S. Ghahfarokhi, "Survey of medium access control schemes for inter-vehicle communications," *Computers & Electrical Engineering*, vol. 64, pp. 450–472, 2017.

[8] R. Bauza and J. Gozálvez, "Traffic congestion detection in large-scale scenarios using vehicle-to-vehicle communications," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1295–1307, 2013.

[9] A. Aliedani and S. W. Loke, "Cooperative car parking using vehicle-to-vehicle communication: An agent-based analysis," *Computers, Environment and Urban Systems*, p. https://doi.org/10.1016/j.compenvurbsys.2018.06.002, 2018.

[10] M. Wang, "Infrastructure assisted adaptive driving to stabilise heterogeneous vehicle strings," *Transportation Research Part C: Emerging Technologies*, vol. 91, pp. 276–295, 2018.

[11] K. Z. Ghafoor, K. Abu Bakar, J. Lloret, R. H. Khokhar, and K. C. Lee, "Intelligent beaconless geographical forwarding for urban vehicular environments," *Wireless networks*, vol. 19, no. 3, pp. 345–362, 2013.

[12] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Generation Computer Systems*, p. https://doi.org/10.1016/j.future.2017.12.041, 2018.

[13] A. Fernández-Isabel and R. Fuentes-Fernández, "Analysis of intelligent transportation systems using model-driven simulations," *Sensors*, vol. 15, no. 6, pp. 14 116–14 141, 2015.

[14] S. Harrabi, I. B. Jaafar, and K. Ghedira, "A Novel Clustering Algorithm Based on Agent Technology for VANET," *Network Protocols and Algorithms*, vol. 8, no. 2, pp. 1–19, 2016.

[15] K. Grover, A. Lim, S. Lee, and Q. Yang, "Privacy-enabled probabilistic verification in broadcast authentication for vehicular networks," *Ad Hoc and Sensor Wireless Networks*, vol. 32, no. 3–4, pp. 239–274, 2016.

[16] W. I. Khedr, "Improved Lightweight Authentication Scheme for IEEE 802.11 p Vehicle-to-Infrastructure Communication," *Adhoc & Sensor Wireless Networks*, vol. 31, no. 1–4, pp. 227–258, 2016.

[17] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking." *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[18] R. Kasana, S. Kumar, O. Kaiwartya, W. Yan, Y. Cao, and A. H. Abdullah, "Location error resilient geographical routing for vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 11, no. 8, pp. 450–458, 2017.

[19] S. Dalya Khalid, K. Omprakash, A. Abdul Hanan, Y. Cao, H. Ahmed Nazar, and K. Sushil, "Location Information Verification using Transferable Belief Model for Geographic Routing in VANETs," *IET Intelligent Transportation Systems*, vol. 11, no. 2, pp. 53–60, 2017.

[20] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[21] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE access*, vol. 3, pp. 343–357, 2015.

[22] C. Wuthishuwong, A. Traechtler, and T. Bruns, "Safe trajectory planning for autonomous intersection management by using vehicle to infrastructure communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 33, 2015.

[23] R. Sun, J. Hu, X. Xie, and Z. Zhang, "Variable speed limit design to relieve traffic congestion based on cooperative vehicle infrastructure system," *Procedia-Social and behavioral sciences*, vol. 138, pp. 427–438, 2014.

[24] R. Kala, "Reaching destination on time with cooperative intelligent transportation systems," *Journal of Advanced Transportation*, vol. 50, no. 2, pp. 214–227, 2016.

[25] A. Bhargava, S. Verma, B. K. Chaurasia, and G. Tomar, "Computational trust model for internet of vehicles," in *Information and Communication Technology (CICT), 2017 Conference on*. 3-5 Nov. 2017, Gwalior, India: IEEE, 2017, pp. 1–5.

[26] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the ratee: A trust management system for social internet of vehicles," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[27] W. He, G. Yan, and L. Da Xu, "Developing vehicular data cloud services in the iot environment," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1587–1595, 2014.

[28] A. Mansoori and C. Achar, "Smart roads using iot devices," *International Research Journal of Engineering and Technology*, vol. 5, no. 6, pp. 1526–1529, 2018.

[29] E. Karaaslan, M. Noori, J. Lee, L. Wang, O. Tatari, and M. Abdel-Aty, "Modeling the effect of electric vehicle adoption on pedestrian traffic safety: An agent-based approach," *Transportation Research Part C: Emerging Technologies*, vol. 93, pp. 198–210, 2018.

[30] K. Małecki, "A computer simulation of traffic flow with on-street parking and drivers' behaviour based on cellular automata and a multi-agent system," *Journal of Computational Science*, vol. 28, pp. 32–42, 2018.

[31] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.

[32] I. García-Magariño, G. Palacios-Navarro, and R. Lacuesta, "TABSAOND: A technique for developing agent-based simulation apps and online tools with nondeterministic decisions," *Simulation Modelling Practice and Theory*, vol. 77, pp. 84–107, 2017.

[33] M. Niazi and A. Hussain, "Agent-based tools for modeling and simulation of self-organization in peer-to-peer, ad hoc, and other complex networks," *IEEE Communications Magazine*, vol. 47, no. 3, 2009.

[34] I. García-Magariño and R. Lacuesta, "ABS-TrustSDN: An agent-based simulator of trust strategies in software-defined networks," *Security and Communication Networks*, vol. 2017, pp. Article ID 8 575 842, 9 pages, https://doi.org/10.1155/2017/8 575 842, 2017.