Owner Identity Verification in the Internet of Connected Vehicles: Zero Trust Based Solution

Mashrukh Zayed, Adnan Anwar, Ziaur Rahman, Sk. A. Shezan, and Rafiqul Islam

***Abstract*—On the Internet of Connected Vehicles, a vehicle has to communicate bi-directionally with several devices for establishing a shared network for inter-vehicle and intra-vehicle connectivity. These connection protocols are commonly structured to connect all the individual components with an implicit degree of trust, which is supposed to protect the whole system from unauthorized users. Technologies like Automotive Ethernet tend to increase security by reducing the implicit trust within the local network devices. However, the lack of individual security protocols in vehicle-to-vehicle communication still keeps the possession of vulnerability to hacks, external attacks, and further disruption. This is where Zero Trust Architecture can become a reliable technology for the exchange of information in between vehicles. Zero trust is a security system that means no one is trusted by default and verification is required from anyone or any device willing to get connected to the intra-vehicle network. In this paper, we have scoped the preliminary and most vital step of this system: verifying the owner identity of a vehicle with zero trust manner. Our approach involves recognizing vehicle license plates and utilizing the license information for retrieving the vehicle owner details to establish trust before allowing connection to the network. Our proposed methodology operates with 85% to 99% accuracy on the license recognition part within recognizable distances using PyTesseract OCR. Reliability to the zero trust solution is gained through necessary information retrieved using GET and POST requests to and from the corresponding driving license information databases.**

***Index Terms*—Connected vehicles, Zero trust, license verification, owner identification, YOLOv4, PyTesseract OCR, GET/POST request**

I. Introduction

THE world we live in is approaching a level of maturity that gives many countries the confidence to implement Smart Cities. With such advancement, a concept related to moving around the city such as Intelligent Transport Systems (ITS) comes to the fore. Smart Cities require contemporary pervasive and dynamic topologies and architectures to achieve spatial intelligence which is supported by ITS. In such systems, vehicles can communicate with one another using Vehicle-to-Vehicle (V2V) communication models. V2V requires the availability of information on demand and anytime; also, that this information must be accessible in real-time by the vehicles as they traverse through the city. This has resulted in a rapid increase in demand for modern vehicles being connected through the Internet, which can be referred to as the Internet of Connected Vehicles (IoCV). With the recent rapid advancement of the Internet of Things (IoT) and future autonomous driving expectations, the IoCV has attracted worldwide attention.

When the on-road vehicles are prompted to connect with the surrounding vehicles through the internet, several issues must be considered before establishing a connection. It is known that the integrity of personal data is the most important attribute to ensure our security in the current digitized world. The evolved IoCV in the smart city context is in a process of ensuring the exchange of information that is necessary to assure safety measures on roads. However, uncontrolled and unauthorized information flow may lead to the possibility of losing personal information and the loss of control over the vehicle or host. Any external device connected to the vehicle can obtain access to the in-vehicle information via Wi-Fi, Bluetooth, or OBD interfaces. Any breach of this information can endanger commuters' lives on the road and social loss in personal life also.

To avoid the consequences related to information privacy, trust, and security, a well-defined trust model before establishing a connection is of primary concern in IoCV. Users' privacy must be protected, as information exchanged between vehicular nodes contains private information about the driver and the vehicle. So, the control authority should be able to identify the driver's liability while at the same time preserving the driver's privacy. Considering these perspectives, trust has become more important than ever. Trust has many meanings across different disciplines, however, trust in vehicular networking

implies reliable multiparty connectivity between vehicles. It narrates the state to which a vehicle accepts information flow with the other vehicles on the network. Therefore, any vehicle prompted for getting connected to the vehicular network has to provide a notion about its condition and identity such as the correctness of ownership data, registration validation, vehicle-fitness details, and other relevant information.

The zero trust architecture can be considered in this context. Zero trust is a security system that means no one is trusted by default and verification is required from anyone or any device willing to get connected to the intra-vehicle network. This architecture doesn't trust a device even if it belongs to its own managed corporate network such as corporate LAN. Connection is not granted even if a device was previously verified. At all costs, the zero-trust approach advocates mutual authentication, including checking the identity and integrity of devices without respect to location and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication. These features can help with the diverse trust issues in IoCV, whether the attack may come from a corporate environment, malicious users, or stolen vehicles.

In this paper, we have scoped the preliminary and most vital step of this system: verifying the owner identity of a vehicle with zero trust manner. Our approach involves recognizing vehicle license plates and utilizing the license information for retrieving the vehicle owner details to establish trust before allowing connection to the network. Reliability to the zero trust solution is gained through necessary information retrieved using GET and POST requests to and from the corresponding driving license information databases. The main contributions of this paper are as follows:

1) Instead of verifying after getting connected over LAN, we focused on individual verification before establishing connection with zero trust manner by utilizing the vehicle license information and owner identity verification.

2) Instead of relying on the network security protocols for the whole security measurement, we built our system with the more secure verification system using GET and POST request to and from the driving license information database.

3) Instead of vehicles getting connected to a dedicated network, we allowed the vehicles to establish own neighborhood clustering for a secure communication with authentic users.

The rest of this paper is organized as follows: In Section II, we review more related works. In Section III, the privacy and security concerns in IoCV and in this work is briefly described and our proposed solution of using zero trust approach is discussed in details. In Section 4, an evaluating experiment for the our proposed method is conducted and discussed. In Section 5, the possible drawbacks of our system is depicted. Finally, Section 6 presents the conclusions and future work resulting from this study.

II. Literature Survey

Researchers have been moving forward with diverse approaches to design a secure vehicular network architecture to solve the information security problem of the vehicle-to-vehicle communication network under the IoCV environment. Although the past works on privacy issues provide security guarantees at different levels, most of the works are limited to applications where communication parties are trusted without verification and there is no authenticity between the vehicle users on the communication network.

One of the most primitive surveys on the privacy and security issues in connected vehicles was performed by T. Zhang et al. [11] in 2014. This study was concerned and confined to the malware attacks on ECUs in specific vehicles. L.B. Othmane et al. [12] (2015) and S. Parkinson et al. [13] (2017) presented two other surveys in later years on different threats in connected vehicles, depending on several communications aspects and vulnerabilities.

The further challenges in connected vehicles associated with IoT have been surveyed recently by several researchers. In a book published in 2020 on "Connected vehicles in the Internet of Things", M. Obaidat et al. [14] discussed current challenges in securing VANETs while A. Modal et al. [15] elaborated about low overhead digital watermark-based vehicle revocation scheme to identify and revoke attackers. Walter et al. [16] (2020) surveyed the influence of data disclosure on vehicle owner-usage intention. A detailed survey on all the existing privacy-enhancing technologies (PETs) and their

limitations was carried out by Safa et al. [17] in the same year.

Along with the survey works, remarkable works have been done by several researchers on implementing secure communication architectures in IoCV. The famous work of M. Amadeo et al. [1] (2016) introduced the features of information-centric networking for connected vehicles. P. Sharma et al. [2] (2017) developed AI filters using the combination of OMNET++ and SUMO for securing wireless communication between vehicles. Few other security architectures like SPBAC Model [4], malware defense for ECUs [5], use of RSUs and Vcash [6], adding correlated noise in the vehicle's IoT layer [7], weight-associated importance-performance using fuzzy multi-criteria decision-making [8] were noticeable for working with the security concerns in IoCV.

Considering the vehicle authentication mechanisms in IoCV, notable work was done by M. Ashritha et al. [19] in 2015. They proposed a lightweight authentication scheme between vehicle to RSU, vehicle to vehicles using the timestamps approach from RSUs. Recently, F. Wei et al. [21] proposed an intelligent terminal-based privacy-preserving multi-modal implicit authentication protocol where they used the password and the vehicle owner's behavior features as the authentication factors.

A tabular presentation of the notable research works related to our literature is presented in Table I along with their concerns, discussions, and propositions.

III. Problem Definition and Solution

A. Privacy and Security Concerns in IoCV

Almost all of the existing V2V technologies imply that a vehicle needs to get connected to the surrounding vehicles using Dedicated Short-Range Communications (DSRC) or cellular radios incorporating RFID technology. These kinds of connections are broadly used for building a dedicated network, known as the Vehicular Ad Hoc Networks (VANETs). However, such connections can not be considered fully reliable considering many safety-critical applications. The fact that there is no connection-wise verification system for every individual vehicle makes it more vulnerable to attacks.

IoCV is more penetrable than VANETs since IoCV is connected to the Internet and the cloud, which increases the number of threats as well as the probability and the severity of an attack launched against it. When a vehicle gets access to a network, it gets connected to all the vehicles in that area, irrespective of being uninformed about the other users. These may lead to different forms of attacks including but not limited to i) Attacks on Authenticity and Identification; ii) Attacks on Confidentiality and Privacy; ii) Attacks on Integrity and Data Trust, etc. [14]. All of these are serious security concerns, considering the increase of malicious users everywhere in the digital world. Even a tiniest minimal connection with an unknown threatening user can cause vulnerability to massive attacks and may lead to life-threatening consequences.

B. Zero-Trust Based Solution

Providing security in vehicular networks is a challenging task due to their high mobility, dynamic topology, and widespread connectivity. Especially, in a dedicated network where users don't get obliged about other existing or entering users, information security and safety becomes highly vulnerable to being misused. Any unknown and unauthentic vehicle may jeopardize the safety of other vehicles, drivers, passengers as well as the efficiency of the transportation system by generating false messages like to clear the road for a selfish reason. Hence identification and authentication of vehicles are essential to protect VANETs from unauthorized message injection and message alteration.

We propose a zero-trust-based solution that requires verification of every single vehicle and its owner before getting connected to the network. The considerably reliable source for this verification can be the vehicle license databases, where both the vehicle and its owner identity are registered. Our methodology is based on (1) detecting the vehicles visible from the car and recognizing the license plate information, (2) using that information for retrieving and verifying the vehicle and owner details by sending GET and POST requests and scrapping the response to and from the vehicle information databases, (3) grant connection if verified, raise alarm if found unauthentic.

TABLE I
LITERATURE SURVEY

Articles	Topics	Discussions & Propositions	Concerns
T. Zhang et al. (2014) [11]	Security and Privacy Issues in IoCV	Identify vehicle-specific challenges, present a cloud-assisted vehicle malware defense framework	Defending vehicles against malware attacks
L.B. Othmane et al. (2015) [12]	,,	Provide a taxonomy on security of communication links, data validity, security of devices, identity and liability, access control	Classify the main threats to connected vehicles
S. Parkinson et al. (2017) [13]	,,	Review large volume of publicly accessible literature based on the vulnerabilities identified	Address the knowledge gaps to minimize future cyber security risks
M. Amadeo et al. (2016) [1]	Secure Communication Architectures proposed in IoCV	Information-centric networking for connected vehicles using named content retrieval, innate multi-cast support, and in-network data caching	Adapt IoCV in extremely dynamic environments
P. Sharma et al. (2017) [2]	,,	AI filters using Context-Adaptive Signature Verification, combination of OMNET++ and SUMO with Veins	Secure wireless communications of Connected Vehicles
Y. Li et al. (2019) [3]	,,	Analyze and summarize the TSP security threats and propose some countermeasures	Enhance ICV security against TSP attacks
M. A. Habib et al. (2019) [4]	,,	SPBAC model for allowing security officials to access information in combination with permissions and roles, instead of roles only	Communication among security layers in a secure, private, and efficient manner
Z. Tian et al. (2020) [6]	,,	Use of RSUs and Vcash for identifying denial of traffic service for connected vehicles	Encourage vehicles to contribute to the traffic event monitoring and verification
S. Ghane et al. (2020) [7]	,,	A differentially private data streaming system that adds a correlated noise in the vehicle's side (IoT layer) rather than the transportation infrastructure	Ensure a strong privacy level over time
M. N. Aladwan et al. (2020) [8]	,,	Fuzzy multi-criteria decision-making algorithm, weight-associated importance-performance analysis	Develop effectiveness and trustworthiness in VC
M. Ashritha et al. (2015) [19]	Vehicle Authentication Mechanism	A lightweight authentication scheme between vehicle to RSU, vehicle to vehicles, timestamps approach	Preserve privacy by not disclosing real identity
F. Wei et al. (2020) [21]	,,	Intelligent terminal based privacy-preserving multi-modal implicit authentication protocols using vehicle owner's behavior features	Protect the security of the intelligent terminal in IOV

IV. PROPOSED METHODOLOGY

A. License Plate Recognition

The very first step of our methodology is to detect vehicles on the road and then detect the license plates using the YOLOv4 algorithm. Then we took the bounding box coordinates from YOLOv4 detection and cropped the sub-image region within the bounds of the box. Since most license plate images were ought to be very small, the majority of the time we used cv2.resize() to blow the image up to 3x its original size. Then, after several stages of smoothing, thresholding, dilation, contouring, and masking, it is passed to Tesseract to get the letter or number from it.

B. Vehicle Owner Identity Verification

1) Sending GET request: In order to retrieve the information from the respective vehicle information database for knowing your vehicle details, the first step is to send a get request using Python "requests" library to the website for downloading the captcha image and using OCR on the captcha image with the help of PyTesseract, the output of PyTesseract is used for bypassing the captcha on the website. This step also uses web scraping using BeautifulSoup to retrieve a randomly generated JavaScript value which is required as a hidden form parameter while

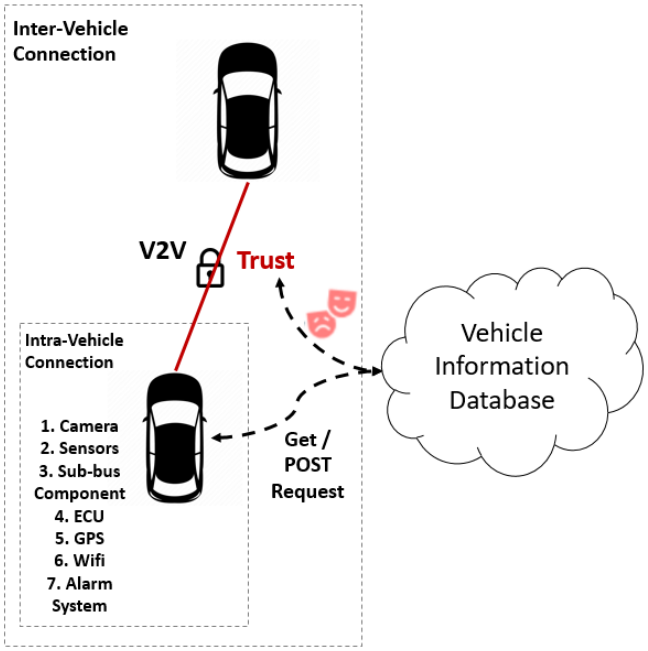

Fig. 1. Trust Establishment Model.

sending Post requests in the next step to identify bots.

2) Sending and Scrapping POST request: After bypassing the captcha, the vehicle license plate number and bypassed captcha strings are passed as form inputs along with randomly generated JavaScript values to generate the POST-request-response.

The POST request response is then scraped and converted into human-readable form by scraping through python library BeautifulSoup.

3) Verifying the retrieved information: If the vehicle license information under consideration is registered in its respective database, the POST-request-response sends the basic information about the vehicle and its owner, which can be considered enough to verify the owner's identity. On the other hand, if the vehicle details are not found in the database, or if any information is found authentic, it raises an alarm and sends a warning to the surrounding vehicles in the network through the vehicle that was verifying.

C. Zero-Trust: Verify Every Connection

This is the most vital part of providing security to the individual vehicles on the streets. Zero-trust refers to trusting no one without verification. We propose this notion of verifying each vehicle while getting connected to each other and to the vehicular network. How this works is described below:

1) A vehicle first detects another vehicle and its license plate that is visible to the camera setup it uses, ie. car dash camera, rear-view camera.

2) It then verifies all the vehicles and their owner identity (Section 4.1 & 4.2) that are visible through its camera setup. After verification, a trusted connection is set up with all of them.

3) Considering the vehicles that are not visible, for getting connected to the network, they must be visible and trusted by any of the vehicles that have already established trust in the network. However, that trust will not allow that unseen vehicle to get connected to all the vehicles in the network. It must get verified by each individual vehicle separately. Hence, the zero-trust methodology is established. We can demonstrate the scenario using the scenario in Figure 3.

Suppose Vehicle 1 (V1) has arrived on the road and wants to connect to its surrounding vehicles as well as the vehicular network. Now, if V1 has two cameras in the front and back, it will be able to verify the authenticity of V2, V3, V6, V7 ie. that are visible to its camera. However, V5 is most likely not visible to V1, so, V1 doesn't know about the existence of V5, nor does V5 itself. So, V1 will not primarily prompt for getting connected to V5 or vice versa. Until this point, we can refer to the currently connected vehicles to V1 as Degree 1 (D1) connections.

Now, what will happen is, V1 will receive information about all the nearest connected vehicles from its D1 connections. This means V1 receives information about all the D1 connections from its own D1 connections. Although these unseen vehicles are trusted by their surroundings, the connection with V1 is not established automatically. V1 will authenticate the license information (Section 4.1 & 4.2) about the unseen vehicles received from its D1 connections. The verified vehicles at this stage will get connected to V1 and vice versa. These connections can be referred to as Degree 2 (D2) connections.

The next stages will go on similarly, where every stage requires authentication of all the vehicles under consideration. We can imagine these level-wise connections as a tree growing all sides that are visual from every level, hence creating a

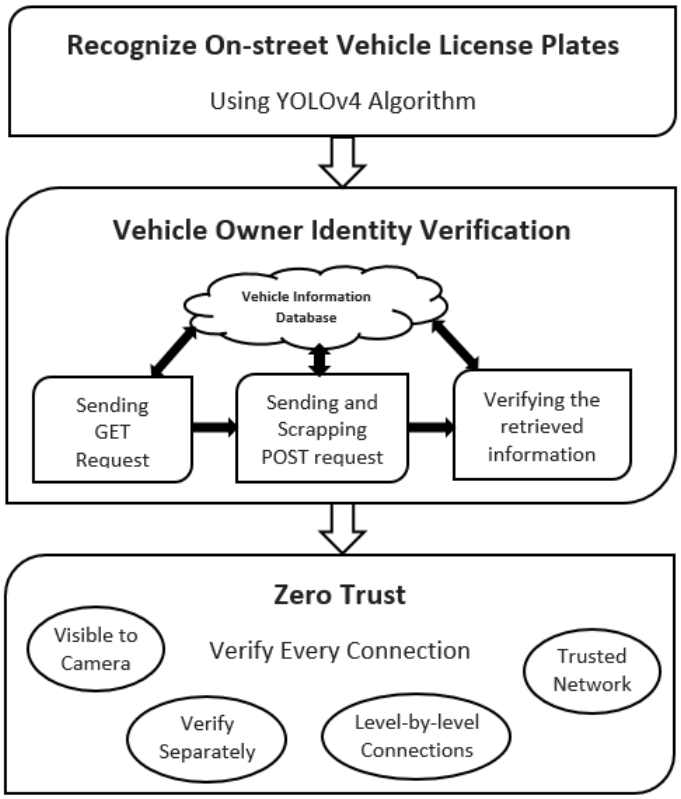

Fig. 2. System Architecture.

Fig. 3. Demo evidence of recognizing license information.

trusted vehicular network.

V. Result Analysis

A. License Plate Recognition Accuracy: Metered Distance

The prior stage of our methodology was detecting and recognizing on-street vehicle license plates using the YOLOv4 algorithm and PyTesseract. Our approach included considering the vehicles that are visible to the camera setup it uses. Our analysis

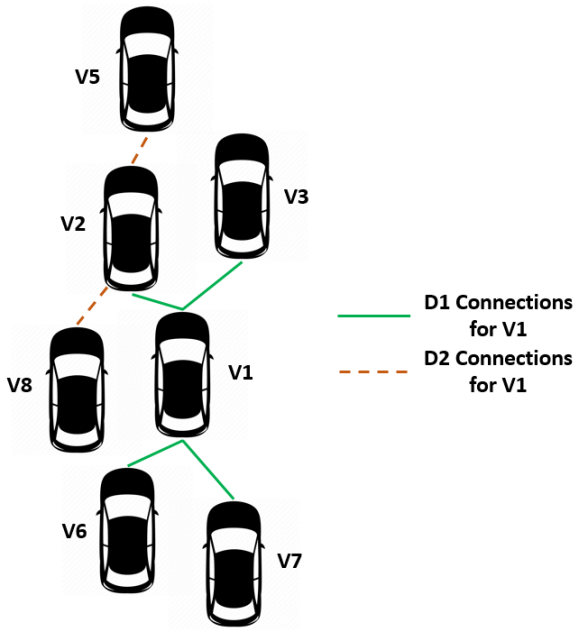

Fig. 4. Neighborhood Cluster for a Vehicle.

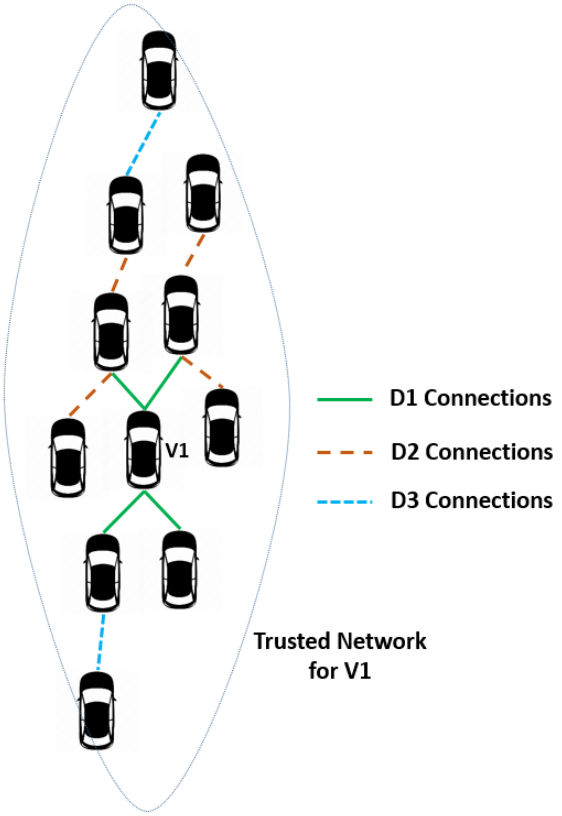

Fig. 5. Trusted Network for a vehicle.

found that distance is another variable that is highly dependable on both the detection and recognition tasks. Table II depicts the recognition performances over metered distances from car dash cameras.

The above table clearly shows that recognizing vehicles would only be fully accurate if they are within a 5-meter distance of visibility from the car dash camera. Hence, in order to get connected to a vehicular network, a vehicle has to be seen within a 5-meter distance of another car that is already connected to the network.

B. Time Perspective for the Identity Verification

After recognizing a vehicle, identifying its license information is a crucial part. Our methodology was to verify that information through GET & POST requests from the vehicle information database. According to Section 4.2 above, this task is performed in three steps, which require a considerable amount of time. Our experimental results showed that the whole verification process can be completed within 10 seconds for all the vehicles in Degree 1 connection. Degree 2 connections require 3 seconds additionally as they are first needed to be received from the Degree 1 connections. Similarly, the next degree connections are made accordingly, which can be seen in Table III.

Each time a vehicle is added to an established network, it gets connected to all the vehicles in that network individually, but at different degree levels. The time required for getting connected is dependent on which degree level the car is getting connected to.

VI. Conclusion

The advent of connected vehicles into the field of IoT has revolutionized so many domains, especially smart vehicles and smart cities. However, information security and privacy protection are still two serious challenges to be addressed and yet to be solved in these domains. With Zero Trust becoming one of cybersecurity's latest buzzwords, it is imperative to understand how Zero Trust can be implemented in the IoCV domain. In this research work, we presented a possible and efficient way of implementing the zero-trust security architecture in the IoCV domain with the help of some latest state-of-the-art detection and recognition mechanisms. We explained that with all the security and privacy concerns along with the counter-measures kept in mind, building a communication network with a zero-trust manner should be the primary concern in this field. We proposed the vehicle owner identification mechanism using automated web scraping requests from corresponding vehicle information databases for establishing that authenticity among the vehicles in the vehicular network. The distance constraint and time perspective of our proposed approach are clearly understandable and can be highly compatible for implementing the methodology at large in real life. Overall, our study indicates that the Zero Trust security model can be the main area of focus for generating indefectible security architectures in IoCV and therefore further needed to be explored.

In future works, IoCV will face more advanced techniques of V2V communication schema along with zero trust methodologies, which will bring the world closer to implementing smart cities in an entirely secured environment for the smart vehicles on our streets.

TABLE II
DETECTION AND RECOGNITION ACCURACY ON METERED DISTANCES

Metered Distance	Detection Accuracy	Recognition Performance
1m - 5m	85 - 96%	accurate
5m - 7m	70 - 80%	not accurate
7m - 9m	50 - 65%	none
¿9m	not detected	none

TABLE III
REQUIRED TIME FOR DEGREE-WISE CONNECTIONS FOR A VEHICLE

Connection Levels	Required Time (seconds)
Degree 1	3s
Degree 2	6s
Degree 3	9s
Degree 4	12s
Degree 5	not determined

REFERENCES

[1] M. Amadeo, C. Campolo and A. Molinaro, "Information-centric networking for connected vehicles: a survey and future perspectives," in IEEE Communications Magazine, vol. 54, no. 2, pp. 98-104, February 2016, doi: 10.1109/MCOM.2016.7402268.

[2] P. Sharma, Hong Liu, Honggang Wang and Shelley Zhang, "Securing wireless communications of connected vehicles with artificial intelligence," 2017 IEEE International Symposium on Technologies for Homeland Security (HST), 2017, pp. 1-7, doi: 10.1109/THS.2017.7943477.

[3] Y. Li, Q. Luo, J. Liu, H. Guo and N. Kato, "TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions," in IEEE Wireless Communications, vol. 26, no. 3, pp. 125-131, June 2019, doi: 10.1109/MWC.2019.1800289.

[4] Habib MA, Ahmad M, Jabbar S, Khalid S, Chaudhry J, Saleem K, Rodrigues JJ, Khalil MS. Security and privacy based access control model for internet of connected vehicles. Future Generation Computer Systems. 2019 Aug 1;97:687-96.

[5] S. Iqbal, A. Haque and M. Zulkernine, "Towards a Security Architecture for Protecting Connected Vehicles from Malware," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1-5, doi: 10.1109/VTCSpring.2019.8746516.

[6] Z. Tian, X. Gao, S. Su and J. Qiu, "Vcash: A Novel Reputation Framework for Identifying Denial of Traffic Service in Internet of Connected Vehicles," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3901-3909, May 2020, doi: 10.1109/JIOT.2019.2951620.

[7] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao and D. Puthal, "Preserving Privacy in the Internet of Connected Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5018-5027, Aug. 2021, doi: 10.1109/TITS.2020.2964410.

[8] M. N. Aladwan, F. M. Awaysheh, S. Alawadi, M. Alazab, T. F. Pena and J. C. Cabaleiro, "TrustE-VC: Trustworthy Evaluation Framework for Industrial Connected Vehicles in the Cloud," in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6203-6213, Sept. 2020, doi: 10.1109/TII.2020.2966288.

[9] M. Han, A. Wan, F. Zhang and S. Ma, "An Attribute-Isolated Secure Communication Architecture for Intelligent Connected Vehicles," in IEEE Transactions on Intelligent Vehicles, vol. 5, no. 4, pp. 545-555, Dec. 2020, doi: 10.1109/TIV.2020.3027717.

[10] Muhammad Haleem Junejo, Ab Al-Hadi Ab Rahman, Riaz Ahmed Shaikh, Kamaludin Mohamad Yusof, Imran Memon, Hadiqua Fazal, Dileep Kumar, "A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks", Scientific Programming, vol. 2020, Article ID 8831611, 21 pages, 2020. https://doi.org/10.1155/2020/8831611.

[11] T. Zhang, H. Antunes and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," in IEEE Internet of Things Journal, vol. 1, no. 1, pp. 10-21, Feb. 2014, doi: 10.1109/JIOT.2014.2302386.

[12] Othmane L.B., Weffers H., Mohamad M.M., Wolf M. (2015) A Survey of Security and Privacy in Connected Vehicles. In: Benhaddou D., Al-Fuqaha A. (eds) Wireless Sensor and Mobile Ad-Hoc Networks. Springer, New York, NY. https://doi.org/10.1007/978-1-4939-2468-4_10.

[13] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898-2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[14] Obaidat M., Khodjaeva M., Holst J., Ben Zid M. (2020) Security and Privacy Challenges in Vehicular Ad Hoc Networks. In: Mahmood Z. (eds) Connected Vehicles in the Internet of Things. Springer, Cham. https://doi.org/10.1007/978-3-030-36167-9_9.

[15] Mondal A., Mitra S. (2020) Security Issues in Vehicular Ad Hoc Networks for Evolution Towards Internet of Vehicles. In: Mahmood Z. (eds) Connected Vehicles in the Internet of Things. Springer, Cham. https://doi.org/10.1007/978-3-030-36167-9_10.

[16] Jonas Walter, Bettina Abendroth, On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services, Telematics and Informatics, Volume 49, 2020, 101361, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2020.101361.

[17] Safa, NS, Mitchell, F, Maple, C, Azad, MA, Dabbagh, M. Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities. Trans Emerging Tel Tech. 2020;e4173. https://doi.org/10.1002/ett.4173.

[18] Maxim Raya and Jean-Pierre Hubaux. 2005. The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN '05). Association for Computing Machinery, New York, NY, USA, 11–21. DOI:https://doi.org/10.1145/1102219.1102223.

[19] Ashritha M and Sridhar C S, "RSU based efficient vehicle authentication mechanism for VANETs," 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), 2015, pp. 1-5, doi: 10.1109/ISCO.2015.7282299.

[20] Dolev, S., Krzywiecki, Ł., Panwar, N. et al. Dynamic attribute based vehicle authentication. Wireless Netw 23, 1045–1062 (2017). https://doi.org/10.1007/s11276-016-1203-5.

[21] F. Wei, S. Zeadally, P. Vijayakumar, N. Kumar and D. He, "An Intelligent Terminal Based Privacy-Preserving Multi-Modal Implicit Authentication Protocol for Internet of Connected Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 3939-3951, July 2021, doi: 10.1109/TITS.2020.2998775.