Secure and Authenticated Protocols for VANETs

Heena Khanna [a,b], Manmohan Sharma [b] Dhavleesh Rattan [c]

[a] *PCTE Group of Institutes, Ludhiana, Punjab, India*
[b] *Lovely Professional University, Phagwara, Punjab, India*
[c] *Punjabi University, Department of Computer Engineering, Patiala, India*

Abstract

With the ever-growing increase in the number of vehicles on road today, the security of the driver and the passengers has become more crucial and challenging than ever before in history. A secure and authenticated message transmission amongst the vehicles is the desired solution everyone is aiming at. The advancements in digital communication have given a new horizon to Vehicle-Vehicle communication. Nevertheless, authentication and privacy is still an open issue to be addressed in order to have a robust VANET. This survey compiles the contribution by the researchers for a Secure and Authenticate formulation of VANET. Towards the end, we enlist some open issues which can make a base for future research work.

Keywords

V2V communication, Vehicular Communication, Wireless Communication, V2V Network, VANET, Vehicular Network

1. Introduction

Two or more vehicles communicating with each other during their drive on road is stated to be V2V communication [1]. To avoid any probable crash, vehicles connected with each other shares the details about location, directions, swift turns, speed, brakes & also for emergency. Mesh network is used by connected vehicles to send, receive and retransmit signals further to communicate. Range for sending signals is upto 300 meters & signals are sent in omni-diretion creating 30 degrees awareness in the vincity (US Department of Transportation). Dedicated Short Range Communication (DSRC) is used to establish the communication. DSRC is a dedicated wireless communication channel used for automotive usage to establish one way or more short range connections. Federal Communication Commission (FCC) and International Organization Standard (ISO) have approved DSRC. Ad- hoc network thus created as nodes with Vehicle is called as Vehicular Ad-Hoc Network (VANET) which further is a subset of Mobile Ad-Hoc Network (MANET) [2]. This VANET comprises of the moving vehicle as well as stationary infrastructure called as Road Side Units(RSU) [3]. Vehicle communication to any other physical device is another variation in this and termed as Vehicle to Infrastructure. It is also termed as Internet of Vehicles in continuation and parallel to Internet of Things (IoT) [4].

VANET seems to be a promising solution to have secure transportation but it comes with a lot of challenges. There can be multiple types of attacks on various layers of networks which can be categorised in either Active or Passive ones. Most of the attacks are found at Network Layer which is the most crucial to keep the network secure[3], in this survey the authors discusses all the possible attacks in VANET. To say it in a crux form, VANET needs to be secured for privacy, authenticity and shall ensure secure message dissemination [5]against all the mentioned attacks [3].

Algorithms, Computing and Mathematics Conference, August 19 – 20, 2021, Chennai, India.
EMAIL: heena.pkalra@gmail.com (Heena Khanna)
ORCID: 0000-0003-0785-8459 (Heena Khanna)

There are many researchers who have come up with some potential protocols to provide a secure and authenticate VANET which are discussed and compared at length in this survey. The protocols have been clumped according to their core technique and have been elaborated according to their year of proposal. The main focus of this survey is to compile the significant contributions in VANET in the last decade despite of the technology so that it can facilitate the group of researchers who are working in the same direction.

This work is categorized in three major segments. In the first segment, the related surveys have been articulated for their contribution. In the second segment, we categorise the protocols according to their techniques and compare their progress and results. In the last segment we lay down the learning from all the existing protocols and list the potential concerns for future researches.

2. Related Surveys

The research progress in V2V communication has been reviewed by many authors. This section summaries some of the significant researches being done in the last decade.

[5] discusses comprehensively about various privacy preserving and authentication techniques used in Vehicular Ad-Hoc Network. The survey compared the work done in the field of security & authentication based on ID-Based, RSU based Key Authentication, Cryptography based bilinear pairing and smart card based protocols. It also shed light upon the protocols that addressed the overhead in the PKI based methods. Not only that, the work also compared the protocols that use message aggregation & cooperative message authentication including batch verification. The survey concluded that three major areas need the robust solutions namely a) authentication of the messaged as well as the vehicles. b) Secure message dissemination and c) user privacy. [6] unfolds how the progress made in the V2V communication has not only given a modern approach to the Transportation but has given hackers the access to the life of the people travelling in the vehicle. Manifesting the point authors have looked upon all major attacks that have been made in the recent past in sensing, communication and control layers. The authors also presented an extensive study on all prospective attacks in V2X communications giving a contrast of their detection probability, properties and ease of attack. Towards the end paper unfolds various Machine Learning & Blockchain based solutions to deal the aforementioned attacks. [3] categorized the attacks on V2V communication on the basis of the Network Layer, being Active or Passive attack and type of attack. Along with the listing and elaborating the attacks authors talked about the proposed solutions which are given by the researchers for each of the attacks. Moreover, it is concluded that a protocol is required which can deal with all types of attacks and provide a mechanism where a trust system is build amongst the people in the Vehicular Network. [7] grouped the attacks in five security services namely Availability, Confidentiality, Authenticity, Integrity and Non-Repudiation and listed the attacks under them and analyzed the authentication schemes for each one of them. Authors also studied various Network & Mobility Simulators. [8] presented the discussion on various algorithms using Machine Learning as a major contributor in safe and authenticated message transmission in V2V. Authors also discussed that there is a need of an algorithm which not only protect from DoS attacks but covers the damage from other attacks as well.

[9] present survey on the researches being done for wireless communication in Vehicles related to their applications in real life, their corresponding protocols and multiple security issues. Authors have analyzed all the researches for their strengths and weaknesses for future work perspectives. [10] gave a contrast of various security issues over the VANET and listed the proposed solutions to handle those issues. The analysis also mentions some motivation for the future work in the same direction. [11] focused how urbanization is leading to increase traffic in the cities and consequently the need of secure data transmission is highlighted. Moreover the authors logged a range of researches talking about inter transmission o f the packets in multiple models of communication. Routing scalability and reliability can be assured using clustering says [12]. The authors made a taxonomy of the clustering techniques used for selection of cluster head, affiliation and overall management. Not only the

benefits but the shortcomings of the algorithms have also been analyzed. The requirements of modern cars and the security issues and proposed solutions are listed by [13]. Whereas, the importance of Encryption and authentication is highlighted by [14] in their survey where the a comparative study is presented for the existing algorithm for VANET. Working on VANET requires the know-how of various Simulation tools which is studied and analyzed by [15] in their paper. They also gave contrast between various attacks and mechanisms used to deal with them. [16] Emphasizes on the authentication for VANET and therefore did a survey on various schemes available for ensuring the authentication. [17]not only emphasized upon the existing security threats but explores on the possible attacks in future which provides a motivation to the researchers to explore and work on their possible solutions. Countermeasures for priori and prosteriori are discussed and analyzed by [18] and a sketch had been proposed for the same alongside the limitations and tensions in VANET then were elaborated and compared.

Table 1: A summary of all the reviews and surveys

Year	Paper	Survey
2020	[5]	Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs)
2020	[6]	Cyber security challenges in vehicular communications
2020	[3]	A Survey on Security in VANETs
2019	[7]	A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy
2018	[8]	Intelligent and Secure Vehicular Network using Machine Learning
2018	[9]	Vehicular ad-hoc network (VANET): Review
2018	[10]	A systematic review on security issues in vehicular ad hoc network
2017	[12]	A Comparative Survey of VANET Clustering Techniques
2017	[13]	Security and privacy in vehicular communications: Challenges and opportunities
2017	[14]	A review on VANET security attacks and their countermeasure
2016	[15]	Recent Advances in VANET Security: A Survey
2016	[16]	A survey on authentication schemes of VANETs
2012	[17]	Survey on security attacks in Vehicular Ad hoc Networks (VANETs)
2009	[18]	Safety and Privacy in Vehicular Communications

3. Analysis of Existing Work

This section elaborates various researches being done over a decade for secure Vehicle to Vehicle communication. We have categorized the algorithms in specific categories whereas some of the algorithms are common and fall in more than one category.

3.1. Various clustering based algorithm for routing techniques in VANET

There are five different categorisation of VANET routing algorithm on the basis of the area and/or application. They are, Geo cast routing protocol, Cluster based routing protocol, Broadcast routing protocol, Topology based routing protocol and Position based routing protocol. [19] Over the years the researches have proposed various models choosing a specific or a hybrid approach to have an efficient and secure model of

VANET. Out of all these categories, clustering based algorithms have been explored the most and given some significant contribution in VANET. In this section, various clustering routing algorithms have been compared and analyzed.

[20] proposed a location based routing protocol with cluster based flooding for VANET. The performance of this algorithm has considered a positional routing protocol called LORA_CBF and also with two non-positional routing algorithms AODV[21] and DSR [22] . The results showed that the performance of positional based is better than the non-positional ones. [23] came up with a clustering based algorithm with delay tolerance. It worked on route discovery for data dissemination following the clustering techniques. It performed better in terms of cost, overheads , stability of the clusters, packet loss ration and end-to-end delay when compared with [24]&[25].

In [23] clusters are formed on the basis of the average speed of the vehicles whereas [26] grouped the vehicles with long travel time and less deviation in speed is selected as Cluster Head and/or Improved cluster head. Due to the same [26] proved showed lower end-to-end delay as compared to CBLR[27].

[28]shared an improved Genetic algorithm-based route optimization technique (IGAROT) which used K-Means Clustering to remove road anomalies. When the algorithm was compared to GA, IGAROT showed 42.0% , 75.7% and 4.24% better results in high, medium and low car density environment respectively.

Table 2: Various clustering based algorithm for routing techniques in VANET

Year Published	**Paper**	**Technique/Method**	**Focus**	**Strength & Weakness**	**Result**
2004	[20]	Location Routing Algorithm with Cluster-Based Flooding (LORA-CBF)	Route Discovery, Time, End to End Delay, PDR	It is ideal for the dynamically changing topologies, large networks & high mobility.	Analyzed with the non-positional algorithms AODV[21] & DSR [22] with the positional based LORA-CBF and it proved to be a better
2017	[23]	Cluster-based On-demand Delay tolerant routing (CODE)	End to End Delay, Packet Loss Ratio, Routing Overhead, Head Change Ratio, Member Change Ratio	It costs less than [24] & [25] due to the minimum overhead	Performed better than LID[24] & HD[25] in terms of cluster stability
2019	[28]	Improved Genetic algorithm-based route optimization technique (IGAROT)	Received signal Strength, transmit power, frequency and path loss	Prompt notifications of the agencies involved in road maintenance.	The proposed methodology performs better that the conventional genetic algorithm in various car density scenarios
2016	[26]	Vehicle with long travel time and less deviation in speed is selected as Cluster Head//	End-End Delay	Scalable, Efficient and distributed	Has lower end-to-end delay as compared to CBLR

		Improved cluster head			

3.2. Fog Computing Based Algorithms for Security

[29]Discussed about various perspectives of data transmission in Vehicles. The paper analyzed various available models for data transmission like 3G and 4G cellular networks, RSUs, Mobile Cloud Computing etc and also analyzed their shortcomings in terms of expense and availability. They proposed to utilize the idle parked and moving vehicles as both computational and communication vehicles. The huge potential of VFC is taken forward to make V2V communication better. [30]Has worked upon reducing the hand off time and increasing the throughput for the vehicular data transmission in Fog computing. The research proposes a solution called as CVFH – A cross Layered and Neighbouring vehicle aided fast handoff wherein they focussed upon two major strategies to achieve their target of reducing the hand off and increasing the throughput during the high speed of Vehicles and High rate of packet transfer. CVFH suggests that in order to decrease hand off delay the Vehicle can choose the Access Point used by the neighbouring Vehicle. Secondly CVFH suggests that the Vehicle shall carry on with the existing Access Point by the time a new connection is established. The simulations have shown CVFH to be a better performer as compared to IEEE 802.11 [31]Proposed a data dissemination model to address the issues involved in Fog Computing while transferring High Volume and non urgency based data transmission. The research also focuses on the fact that the fog model becomes expensive and how to utilize the fog Based Computing efficiently. Therefore they proposed Delay Tolerable Network(DTN) approach . In this approach they assign different role to Cloud and Fog Severs. Here, the Cloud is given the job to manage data flows & content queries where as the Fog Servers are dedicated to disseminate data using Delay Tolerant Network. The research results showed that their model depicts a higher delivery success ratio and less delay to ensure a better system to disseminate important data in Fog Computing. [32]Initiated to work on a model that creates a layer in between the Vehicle and the server to speed up the data transfer. Just like when the client send a request to the server and cache memory maintains the information for better processing the next time. They have proposed a model called SIVNFC which prevents DoS Attacks across the network. [33]

Have done an analysis to check the data transmission on 28GHz. In order to overcome the problems to high level of interference and High Packet Error they have done a deep interference analysis to derive the right expressions of Packet Error Probability and Ergodic Capacity. The same has been simulated extensively to be proven to next revolutionary step in V2V Communication.

[34] Introduced an intermediary fog layer to improve latency in Vehicle to Vehicle communication. The algorithm works on the efficiency in terms of improving the delay in the messages. To ensure the authentication it used Long Term & Short Term Pseudonym/Keys. [35]integrated hybrid optimization techniques for authentication of the network. It integrated Cuckoo Search Algorithm, Firefly Neural Network, Firefly Algorithm and Key Distribution Establishment in the protocol to ensure the network is prevented from DoS and SNI Attacks. The results showed improved throughput and less jitter. [36]extended the research and introduced the implementation of Artificial Bee Colony (ABC) and Genetic Algorithms to detect real time DoS attacks in IEEE 802.11p. Algorithm is also capable to classify between genuine and attacked vehicles with the help of Feed forward back propagation neural network (FFBPNN). The algorithm proved to give 92% accuracy and reduced the jitter by 72%.

To ensure the safe communication in VANET, trusted authority (TA) comes into the picture. Self authentication amongst the RSU and Vehicles can diminish the burden of TA. [37] proposed a fog based model for anonymous authentication to ensure real time communication and reduced pressure on TA using pseudonym based tracking mechanism to update and track. The algorithm gave promising results in terms of privacy protection & authentication. Where[37] talked about anonymous authentication [38] proposed an algorithm for mutual authentication and generates a secret key for secure communication between two vehicles. It ensures privacy protection and claims practicality for the implementation reducing the communication cost.

Table 2 lists all the Fog Based protocols with their comparison.

Table 3: Fog Computing Based Algorithms for Security

Year Published	Paper	Technique/Method	Focus	Strength & Weakness	Result
2017	[34]	The authors introduce the concept of Fog Computing and used to the concept of LTP/LTK & STP/STK	Security	Latency of key transfer is reduced due to the Fog Node.	Lesser Delay
2019	[35]	A Fog integrated VANET Scheme compared with Firefly and Cuckoo	Security	Prevents the network from DoS and SNI	Throughput 8100 at PIR 0.02 PIR 0.001 to 0.02. Maximum jitter is 96ms
2019	[36]	VFC with Hybrid Optimization Algorithm like Cuckoo, Firefly & ABC	Security	Provides real time detection of HDSA in IEEE802.11p	92% Prediction accuracy . Reduced the jitter by 72%.
2017	[37]	Fog Computing & d pseudonym-based batch anonymous authentication	Anonymous Authentication		Ensured privacy protection and efficient authentication.
2019	[38]	Authenticate Key Agreement without bilinear pairing	Security		Improved Communication & Computation Cost

3.3. ID & Signature Based Algorithms for Batch Authentication

The need of VANET came into the picture when the number of vehicles increased due to urbanization and affordability of vehicles. Initially horns, hand waves and other mediums of traffic controls were sufficient and gradually the traffic police came into the picture. Now, with the advancement of technology & digitization the call for VANET has tremendously increased so as to improvise the transportation system and ensure smooth and safe travel. However, technology always comes with a threat of security & authentication. In order to authenticate the sender of the information various protocols have been introduced. The protocols can be categorized into two heads, individual authentication & batch verification. With the increased number of vehicles, one-to-one authentication becomes impossible & inefficient and therefore the concept of Batch Scheme of authentication proved itself to be more effective [39]. [39] have integrated Bilinear pairing to authenticate the signatures in batch and performance proved the algorithm to be performing better than [40] and is also capable to handle replay and non-repudiation. However, it still lacks when it comes to identifying illegal signatures. To overcome the shortcomings of [39], [41] came up with another algorithm after analyzing the work of [41] and arriving at a conclusion that it lacks the capability to handle impersonation attack. The algorithm is based upon the four step process Key Generation & pre-distribution, pseudo identity generation, message signing and message verification. Bilinear pairing has been recognized as one of the most complex operation when we talk of cryptography in modern times [42]. To provide a better an simpler mechanism a set of researchers have come up with CPAA based schemes without integrating Bilinear pairing. [42] Proposed a scheme which supports privacy protection and mutual authentication at the same time. The proposed scheme could be used for V2I and V2V both. Whereas [43] continued the work on CPAA and integrated One way Hash function and Elliptic Curve Cryptography provide a scheme with lesser cost of computation and communication. To reduce the cost even more [44] suggested to opt for aggregate signature instead of individual signature verification. They integrated Elliptic Curve Cryptosystem. The research results show that the signature verification time has improved from 94.3% to 92.7%.

Table 4: ID & Signature Based Algorithms for Batch Authentication

Year Published	Paper	Technique/Method	Focus	Strength & Weakness	Result
2013	[39]	Batch Scheme based on Bilinear	Authentication	Secure & Efficient.	Compared with [40] and performed better in terms of efficiency

		pairing		Can handle replay attack and non-repudiation	
2014	[41]	Batch Scheme	Authentication		Works on impersonation attack and improved version of [39]
2015	[42]	Conditional Privacy-Preserving Authentication (CPPA) without bilinear pairing	Authentication	Could be used for V2I and V2V both. Easier to deploy	Improved communication & computation cost
2016	[45]	DiffieHellman is used to ensure security & Discrete Logarithmic encryption scheme is used for Cryptography.	Security	Vehicles with thin network are benefitted as it works on secure positioning algorithm.	Improved confidentiality, authentication, access and availability. PDR 98%. End-to-end delay is 0.16
2019	[43]	ID Based Signature Scheme without bilinear paring IBS-CPAA added to Elliptic Curve Cryptography & general one way Hash Function	Authentication		Lower computational cost due to batch signature verification
2018	[44]	Certificate less aggregate signature without pairings	Authentication	Useful for V2I, reduced cost of verification.	Improved communication & computation cost. Reduced computing time. Verification time is 450ms for 1000signatures, improved by 94.3% to 92.7%

3.4. Smart Card Based Algorithms for Authentication & Security

In the last decade Smart Card Based authentication has been explored more than ever before. They have an incredible capacity to hoard enormous amount of data with the help o f embedded circuit chip and memory chip. Smart cards offer a strong security base and have been used in many authentication algorithms, encryption techniques and asymmetric key services. [46]

Researchers have explored Smart Cards authentication capabilities for VANET as well. [47]'s PAAVE generates on-the-fly anonymous keys amongst RSU and the vehicles. Their results show improved efficiency, Communication Overhead and Computational time. [48] continued the work to provide an even more efficient way which not only diminishes the cost but also withstands attacks like offline password guessing attack, smart card loss attack, impersonation attack and some more. [49] proposed Anonymous & light weight scheme for the authentication of User and the message at not only authentication stage but also at password change and data transmission phases as well. The protocol can deal with offline password guessing attack and impersonation attack and also works on Packet loss ratio & latency. All these protocols used Smart Card for anonymous authentication whereas [50] came up with an authentication protocol which uses real identity of the drivers. It uses Spanish eICard and ensured 60-70% correctly obtained identities.

Table 5: Smart Card Based Algorithms for Authentication & Security

Year	Paper	Technique/Method	Focus	Strength &	Result

Published				Weakness	
2010	[47]	PAAVE-Anonymous authentication using Smart Cards	Authentication &Security	Generates the anonymous keys on the fly for vehicle s and RSUs. Vehicle has to store one cryptographic key	Improved efficiency, Communication Overhead and Computational time.
2014	[48]	*Efficient Authentication Protocol* Ensures anonymity by dynamically generated login ids	Authentication & Security	Can resist offline password guessing attack, smart card loss attack, impersonation attack, DOS Attack. Provide anonymity preservation	Improved Computational & Communication Cost.
2017	[49]	*Anonymous & light weight scheme for the authentication of User and the message.* Diffie-Helman protocol; smart cards; hash functions; centralized trusted authority for loading smart-cards with login id and password	Authentication & Security	Can deal with as offline password guessing attack and impersonation attack	More than 50% of Computational & Communication Cost. Works on Packet loss ratio & latency.
2016	[50]	*Obtains the real identities of the drivers through t he Spanish eICards*	Authentication	Improved results shown on the real map during the simulation	In 60-70% of the cases the identity is correctly obtained.

4. Conclusion & Future Scope

Researchers have been working intensely on improving the security mechanism in V2V communication and have proposed various techniques as discussed in this survey. By comparing the work accomplished till date some open issues have been discovered which can be used as a potential input for the future researchers. Firstly, all the cluster based algorithms have been proved to be better than other techniques but the researchers must keep on comparing their work within the domain with other cluster based algorithms. Also, it is assumed that the real time environment has the RSUs and other infrastructure in place which is not the reality. The design complexities while implementation should not be ignored. Apart from Firefly and Cuckoo, spline and polynomial fit could be used for better comparison and improved results. There are very less impressions of researches using IoT in this domain, so that's another prospering field. Implementation of Elliptic Curve cryptography in future to stimulate the identification process to work on location based mechanism is yet another unexplored area. These are few areas where the future researches can be directed and help in achieving the real time solutions.

In this survey we discussed about various algorithms focusing on Secure and Authenticated algorithm under four categories namely Clustering Based, Fog Based, ID Based and Smart Card Based. Towards the end we shared some uncovered topics for future work with a hope that these issues are addressed by the researchers and a potential solution is proposed.

Table 6: Abbreviations

DLIES	**Discrete Logarithm Integrated Encryption Scheme**
DoS	Denial of Service
SNI	Smart & Normal Intrusions
PDR	Packet Delivery Ratio
PIR	Packet Injection Ratio
VFC	VANET-cloud and fog computing
HDSA	Hybrid DoS Attacks
ABC	Artificial Bee Colony
LTP	Long Term Pseudonym
STP	Short Term Pseudonym
LTP	Long Term Key
STK	Short Term Key
TA	Trusted Authority
RSU	Road Side Unit
FFBPNN	Feed forward back propagation neural network
VFC	Vehicular Fog Computing
VANET	Vehicular Ad-hoc Network
CBLR	Cluster Based Location Routing
CPPA	Conditional Privacy-Preserving Authentication
PAAVE	Protocol for Anonymous Authentication in Vehicular Networks (PAAVE)

5. References

[1] L. Wu *et al.*, “An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular Ad Hoc network,” *IEEE Access*, vol. 7, pp. 55050–55063, 2019, doi: 10.1109/ACCESS.2019.2911924.

[2] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETs,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011, doi: 10.1109/JSAC.2011.110311.

[3] T. Pavithra and B. S. Nagabhushana, “A Survey on Security in VANETs,” in *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*, Jul. 2020, pp. 881–889, doi: 10.1109/ICIRCA48905.2020.9182823.

[4] M. N. Tahir, K. Maenpaa, and T. Sukuvaara, “Analysis of SafeCOP features in V2I and V2V communication,” in *IEEE Vehicular Technology Conference*, Apr. 2019, vol. 2019-April, doi: 10.1109/VTCSpring.2019.8746587.

[5] D. Manivannan, S. S. Moni, and S. Zeadally, “Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs),” *Veh. Commun.*, vol. 25, p. 100247, 2020, doi: 10.1016/j.vehcom.2020.100247.

[6] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” *Vehicular Communications*, vol. 23. Elsevier Inc., p. 100214, Jun. 01, 2020, doi: 10.1016/j.vehcom.2019.100214.

[7] Z. Lu, G. Qu, and Z. Liu, “A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 760–776, Feb. 01, 2019, doi: 10.1109/TITS.2018.2818888.

[8] M. Sharma and H. Khanna, “Issue 12 www.jetir.org (ISSN-2349-5162) JETIREC06080 Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir,” 2018. Accessed: Mar. 21, 2021. [Online]. Available: www.jetir.org.

[9] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, “Vehicular ad-hoc network (VANET): Review,” in *2018 IEEE International Conference on Innovative Research and Development,*

ICIRD 2018, Jun. 2018, pp. 1–6, doi: 10.1109/ICIRD.2018.8376311.

[10] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, “A systematic review on security issues in vehicular ad hoc network,” *Secur. Priv.*, vol. 1, no. 5, p. e39, Sep. 2018, doi: 10.1002/spy2.39.

[11] P. Mutalik and V. C. Patil, “A survey on vehicular ad-hoc network [VANET’s] protocols for improving saf[1] P. Mutalik and V. C. Patil, ‘A survey on vehicular ad-hoc network [VANET’s] protocols for improving safety in urban cities,’ in Proceedings of the 2017 International Conference ,” in *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*, May 2018, pp. 840–845, doi: 10.1109/SmartTechCon.2017.8358491.

[12] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, “A Comparative Survey of VANET Clustering Techniques,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 657–681, Jan. 01, 2017, doi: 10.1109/COMST.2016.2611524.

[13] C. Bernardini, M. R. Asghar, and B. Crispo, “Security and privacy in vehicular communications: Challenges and opportunities,” *Vehicular Communications*, vol. 10. Elsevier Inc., pp. 13–28, Oct. 01, 2017, doi: 10.1016/j.vehcom.2017.10.002.

[14] Deeksha, A. Kumar, and M. Bansal, “A review on VANET security attacks and their countermeasure,” in *4th IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2017*, Sep. 2017, vol. 2017-January, pp. 580–585, doi: 10.1109/ISPCC.2017.8269745.

[15] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, “Recent advances in VANET security: A survey,” Jan. 2016, doi: 10.1109/VTCFall.2015.7391111.

[16] E. A. Mary Anita and J. Jenefa, “A survey on authentication schemes of VANETs,” Jul. 2016, doi: 10.1109/ICICES.2016.7518946.

[17] M. S. Al-Kahtani, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs),” 2012, doi: 10.1109/ICSPCS.2012.6507953.

[18] J. Domingo-Ferrer and Q. Wu, “Safety and privacy in vehicular communications,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5599, pp. 173–189, doi: 10.1007/978-3-642-03511-1_8.

[19] R. Kumar and M. Dave, “A Comparative Study of Various Routing Protocols in VANET,” vol. 8, no. 4, pp. 643–648, 2011, [Online]. Available: http://arxiv.org/abs/1108.2094.

[20] R. A. Santos, R. M. Edwards, L. N. Seed, and A. Edwards, “A location-based routing algorithm for vehicle to vehicle communication,” doi: 10.1109/ICCCN.2004.1401632.

[21] S. Das C. Perkins, E. Belding-Royer, “Ad hoc On-Demand Distance Vector (AODV) Routing,” 2003, [Online]. Available: https://tools.ietf.org/html/rfc3561.

[22] D. B. Johnson and D. A. Maltz, “DSR : The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks,” *Comput. Sci. Dep. Carnegie Mellon Univ. Addison-Wesley*, pp. 139–172, 1996, [Online]. Available: http://www.monarch.cs.cmu.edu/.

[23] J. Zheng, H. Tong, and Y. Wu, “A Cluster-Based Delay Tolerant Routing Algorithm for Vehicular Ad Hoc Networks,” in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Jun. 2017, pp. 1–5, doi: 10.1109/VTCSpring.2017.8108461.

[24] R. Sheridan and D. Sheridan, “A design Concept for Reliable Mobile /Radio Networks with Frequency-Hopping Signaling,” 1988.

[25] a Alwan, R. Bagrodia, N. Bameos, M. Gerla, and L. Kleinrock, “Mobile Multimedia Networks,” *Ieee Pers. Commun.*, no. April, pp. 34–51, 1996.

[26] S. Jalalvandi, “A Cluster-Based Routing Algorithm for V ANET A . Ad-Hoc Routing D . Geocast-Based Routing B . Position-Based Routing Cluster-Based Routing Broadcast-Based Routing,” pp. 2068–2072, 2016.

[27] R. A. Santos, R. M. E. Amiee, and N. L. Seed, “Using the CLuster-based Location Routing (CBLR) Algorithm for Exchanging Information on a Motorway,” pp. 0–4.

[28] H. Bello-Salau, A. M. Aibinu, Z. Wang, A. J. Onumanyi, E. N. Onwuka, and J. J. Dukiya, “An optimized routing algorithm for vehicle ad-hoc networks,” *Eng. Sci. Technol. an Int. J.*, vol. 22, no. 3, pp. 754–766, 2019, doi: 10.1016/j.jestch.2019.01.016.

[29] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, “Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016, doi: 10.1109/TVT.2016.2532863.

[30] Y. Bi, “Neighboring vehicle-assisted fast handoff for vehicular fog communications,” *Peer-to-Peer Netw. Appl.*, vol. 11, no. 4, pp. 738–748, Jul. 2018, doi: 10.1007/s12083-017-0570-8.

[31] L. Gao, T. H. Luan, S. Yu, W. Zhou, and B. Liu, “FogRoute: DTN-based Data Dissemination Model in Fog Computing,” *IEEE Internet Things J.*, pp. 1–1, 2017, doi: 10.1109/JIOT.2016.2645559.

[32] K. Sharma and D. Motwani, “FAST Data Dissemination MODEL in VANETs Using FOG.” Accessed: Sep. 24, 2020. [Online]. Available: https://journal.amityaump.com/papers/ETJRI_V1_Issue_2_04.pdf.

[33] O. A. Saraereh, A. Ali, I. Khan, and K. Rabie, “Interference analysis for vehicle-to-vehicle communications at 28 GHz,” *Electron.*, vol. 9, no. 2, Feb. 2020, doi: 10.3390/electronics9020262.

[34] S. Chaba, R. Kumar, R. Pant, and M. Dave, “Secure and efficient key delivery in VANET using cloud and fog computing,” in *2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017*, Aug. 2017, pp. 27–31, doi: 10.1109/COMPTELIX.2017.8003932.

[35] S. K. Erskine and K. M. Elleithy, “Secure intelligent vehicular network using fog computing,” *Electron.*, vol. 8, no. 4, 2019, doi: 10.3390/electronics8040455.

[36] S. K. Erskine and K. M. Elleithy, “Real-Time Detection of DoS Attacks in IEEE 802.11p Using Fog Computing for a Secure Intelligent Vehicular Network,” *Electronics*, vol. 8, no. 7, p. 776, Jul. 2019, doi: 10.3390/electronics8070776.

[37] M. Han, S. Liu, S. Ma, and A. Wan, “Anonymous-authentication scheme based on fog computing for VANET,” *PLoS One*, vol. 15, no. 2, p. e0228319, Feb. 2020, doi: 10.1371/journal.pone.0228319.

[38] M. Ma, D. He, H. Wang, N. Kumar, and K. K. R. Choo, “An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8065–8075, Oct. 2019, doi: 10.1109/JIOT.2019.2902840.

[39] C. C. Lee and Y. M. Lai, “Toward a secure batch verification with group testing for VANET,” *Wirel. Networks*, vol. 19, no. 6, pp. 1441–1449, 2013, doi: 10.1007/s11276-013-0543-7.

[40] C. Zhang, P. H. Ho, and J. Tapolcai, “On batch verification with group testing for vehicular communications,” *Wirel. Networks*, vol. 17, no. 8, pp. 1851–1865, 2011, doi: 10.1007/s11276-011-0383-2.

[41] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, “A secure authentication scheme for VANETs with batch verification,” *Wirel. Networks*, vol. 21, no. 5, pp. 1733–1743, 2015, doi: 10.1007/s11276-014-0881-0.

[42] D. He, S. Zeadally, B. Xu, and X. Huang, “An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2681–2691, 2015, doi: 10.1109/TIFS.2015.2473820.

[43] I. Ali, T. Lawrence, and F. Li, “An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs,” *J. Syst. Archit.*, vol. 103, p. 101692, 2020, doi: 10.1016/j.sysarc.2019.101692.

[44] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, “An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks,” *Inf. Sci. (Ny).*, vol. 451–452, pp. 1–15, 2018, doi: 10.1016/j.ins.2018.03.060.

[45] T. Limbasiya and D. Das, “Secure message transmission algorithm for Vehicle to Vehicle (V2V) communication,” *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, pp. 2507–2512, 2017, doi: 10.1109/TENCON.2016.7848485.

[46] K. Mayes and K. Markantonakis, *Smart cards, tokens, security and applications: Second edition*. Springer International Publishing, 2017.

[47] V. Paruchuri and A. Durresi, “PAAVE: Protocol for anonymous authentication in vehicular networks using smart cards,” *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 0–4, 2010, doi: 10.1109/GLOCOM.2010.5683087.

[48] B. Ying and A. Nayak, “Efficient authentication protocol for secure vehicular communications,” *IEEE Veh. Technol. Conf.*, vol. 2015-Janua, no. January, pp. 0–4, 2014, doi: 10.1109/VTCSpring.2014.7022900.

[49] B. Ying and A. Nayak, “Anonymous and lightweight authentication for secure vehicular networks,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, 2017, doi: 10.1109/TVT.2017.2744182.

[50] J. Sánchez-García, J. M. García-Campos, D. G. Reina, S. L. Toral, and F. Barrero, “On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks,” *Futur. Gener. Comput. Syst.*, vol. 64, pp. 50–60, 2016, doi: 10.1016/j.future.2016.04.024.