International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 9 (2020) pp. 884-890

A Location Privacy Framework using Edge Computing in VANET

Om Dukiya [1] and Gajendra Shrimal[2]

Jagannath University, Jaipur, Rajasthan, India.

Abstract

The edge computing model are anticipated to resolve the significant flaws affecting recent trends that demands the cloud computing resources for functioning. Such novel prototypes will be useful for the users as they bridge the computational resources closer. This will enhance the bandwidth utilization and decreases the latency of network, but it will append few impressive context-awareness properties to the respective systems. In this paper, we study how the application of attractive features of edge computing can be utilized to enhance the privacy (location privacy) of the vehicular networks (VN), particularly authentication, revocation and anonymity issues. In general, we observe the existing privacy challenges in the vehicular networks and study the existing deployment models by arranging them into three categories. The outcome states that the computational overhead can be significantly reduced without compromising the privacy of vehicular nodes, if vehicular edge communication established ideally.

Keywords: Vehicular Networks, Privacy, Location Privacy, Anonymity, Edge Computing, Internet of Things.

I. INTRODUCTION

In every country, Transportation Systems are the most prominent asset, which provides us the goods and services that are essential for the well-being of our society. Factors affecting the performance of the transportation system does not only create hurdles in the supply and distribution of various goods and services but may also lead to the loss of human lives. As we know that many people get injured and lose their lives every day in road accidents. Due to this reason, road safety is considered as one of the most promising applications of the intelligent transportation systems (ITS)[1]

To provide better security and safe road management in our transportation system, we can utilize a communication infrastructure known as vehicular networks (VN) [2]. Vehicular networks are fundamentally developed to reduce the risk of accidents and road fatalities by using safety or alert messages. These safety messages carry essential information about the vehicle and its driver[2].

Due to the broadcast nature of such messages and the demand for real-time information to alert the other vehicles, these messages generally travel without encryption. Although it is mandatory to authenticate the sender of these messages whenever an alert message is received, to hinder from malign entities from inserting the false data, this may not only create small traffic congestion but may lead to car accidents.

The major challenge of VN is to authenticate the data senders successfully. In order to resolve this issue, many authentication approaches have been proposed by various security standards. Few of them are IEEE 1609.2 and ETSI TS 102 941, generally known as public key infrastructure (PKI) as in our existing networking systems. Other ITS security standards are currently under-development states, such as ISO/CD TR 17427-5, ISO/AWI TS 21177, and ISO/AWI

TS 21185, however, no further details are confirmed through which authentication can be achieved.

Hence, in recent standards, apart from issuing digital certificates used by vehicles to send along with the messages for authentication, the role of PKI is to manage the issuance, renewal, and revocation of the certificates(revoked certificates entry is maintained in certificate revocation list i.e. CRL). Before considering a message as a primitive or valid message, it is mandatory to check its certificate credentials in the CRL, as this would declare the malicious behavior of the vehicle. As we know, the retrieval and management of these bulky CRLs is the most obvious reason for not using the PKIs for authentication in VN, and this demands alternative solutions[3]. However, none of them can effectively solve the priorly mentioned issues.

As we will explain later, the communication model is extremely significant to the challenges faced by VN. Besides, not only the authentication of the messages is an important issue but preserving location privacy and identity privacy of a vehicle is equally important. If the sender vehicle can be authenticated, we can achieve the location privacy and keep the identity of the vehicle owners private. However, another dilemma is vehicle owners will act hesitant to reveal their location and identity while communicating with the other VN entities.

It is prototype shifting and a huge favor is drawn from different industries and Consortiums (such as Nokia, IBM, Cisco, etc.) to brings the opportunity of using Multi-access Edge Computing (MEC) to overcome the problems encountered so far. MEC provides an IT service environment and cloud-computing capabilities at the edge of vehicular networks. Thereafter, V2V communications may not be the absolute solution for location privacy and existing deployment

generally degrade the prior belief that applications with real-time needs to follow the inter-vehicular communications.

Accordingly, in this paper, we focus on the Vehicular Networks location privacy and identity preservation challenges(such as anonymity, authentication and) can be handled by the edge technologies and analysis of how these privacy frame- works can be unified on Vehicular Edge Computing (VEC) without depending fully on inter-vehicle communications. We extend this analysis part to a step forward, by discussing the privacy challenges of edge-enabled VN and states considerate solutions for the respective problems.

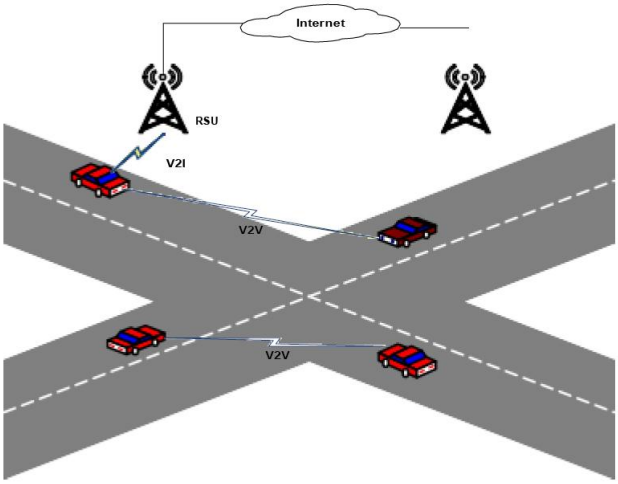

Fig. 1. An Example of simple Vehicular Network

The organization of the paper is as follows. In the second section, we provide background information on vehicular networks and edge computing keeping in mind their similarities and differences. Further in section III, we will present a literature review that focuses on privacy challenges in vehicular networks. Section IV presents our possible deployment models and their description. In the last, Section V provides an analysis of how VEC can help in solving the existing privacy problems mentioned in Section III. The conclusions of this paper are presented in Section VI.

II. BACKGROUND

A. Vehicular Networks

Vehicular networks are considered as the most fundamental block of Intelligent Transportation Systems (ITS) and Internet of Vehicles(IoV). As compared to the traditional sensor networks and existing ad-hoc networks, VANET faces a new set of challenges. In the existing research work, several definitions are present to define vehicular ad-hoc networks. In this work, we describe a vehicular network attempting to present every feature converged by the existing studies while featuring the unique characteristics of it.

A vehicular network consists of moving vehicles, these vehicles communicate with each other using vehicle-to-vehicle (V2V), and may use roadside infrastructure vehicle-to-roadside units(V2R), to gain the information about road safety and entertainment applications. Such communication can be established using various cellular technologies(LTE and WiMAX). A significant feature of vehicular networks is that vehicles are highly dynamic in nature and the infrastructure contains static nodes, refer Fig for a clear understanding of the environment.

In vehicular networks, nodes are equipped with on-board units (OBU) which provides limited but ample computing and storage facilities. This OBU is internally connected with the different sensor units installed in the vehicle (such as front and rear navigation cameras, radars, airbags, the pressure of the tire, wheel rotation and speed sensors, etc.). In vehicular networks, RSU is static nodes or fixed nodes that are located at a specific distance/range of the vehicles[4]. It is hard to establish the communication between static and dynamic nodes in vehicular networks, but we have different ITS standards(e.g. ISO 21217:2014 name them CALM, etc) to support the communication in the network.

Both the cellular-based vehicular to vehicular networks(like C-V2X) and other technologies such as 802.11p utilizes the specially designed vehicular protocols to gain the services, like broadcasting of the safety messages in the environment. From the set of these dedicated protocols, one most popular is DSRC/ WAVE stands for dedicated short-range communication/ Wireless access for the vehicular environment. The whole communication is established by regularly broadcasting authenticated beacon messages. This continuous broadcasting of the beacons which carry information about the vehicle and its driver may endanger the privacy of the vehicle's user. Therefore, we need a dedicated protocol to manage the privacy of the user and their vehicle[5].

Existing vehicular network models generally contemplate a simple communication model suitable for the V2V environment. This traditional model considers the scenario in which vehicles can communicate with each other without the interference of static RSUs. This does not only include communication between neighboring nodes but also multi-hop communications using the benefits of inter-mediate nodes as relays. Such type of V2V communication is considered as the paramount when there is no static device available. Although, this type of communication creates complexity in the authentication process and privacy issues become more sensitive[6].

B. Edge Computing

Edge computing is developing as a promising technology that focuses to decentralize the cloud services by integrating the transmission, increasing storage and computation capability. The fundamental aim of edge computing is to distribute the capabilities of cloud to real things. This does not only enhance user experience, because of the decrease in network latency and the less response time of the system. It will also reduce the bandwidth consumption between the edge and centre of the network, where computational capabilities are built in traditional cloud environment[7].

However, we can assume that Edge computing can act as the development of the cloud computing. Edge computing cannot work without the coincide of cloud computing. The architecture is a three layer model consists of vehicular nodes(end-user devices), Edge layer and Cloud-server layer.

a. Vehicular Nodes: The node of this environment(RSU and vehicles) act as end user of the model and known as the clients of the architecture. These nodes work ideal with the support of edge computing. These devices includes available smart devices such as smartphones, wearable, pre-installed sensors, and almost every devices that has computational capabilities in any aspect.

b. Edge Layer: This layer works on the top of first layer and provide the support to the nodes for faster computational services. We can refer edge layer as mini-cloud server that is available at various locations and manage network and hardware demand of the environment. Such Facilities can be deployed in the cellular tower, traffic signals, gateways, routers and so on.

c. Cloud Server layer: At this layer, we have distinctly powerful computers deployed at a remote location, to provide services to the second layer. The important aspect is that internal layer of the architecture may consist of a number of layers of various type of devices. Generally, these highly capable devices are utilized for co-ordination and assembly purpose to keep the backup of previous and recently collected information. Although, the edge technology is considered as a self-dependent and does not completely rely on the existence of upper-layer devices.

As we have mentioned in the above section, we follows that edge computing model and our VN share various similar features in terms of development. Nevertheless, the implementation of edge computing demands a prior introduction of few challenging technologies such as (SDN, 5G, NFV, etc.), which are not currently available in our traditional networks. Also the availability of these technologies are effective in enhancing the bandwidth utilization, network latency and reduction in the response time of the VN[1].Hence, the edge computing is appropriate technology to meet the specific requirements of vehicular networks in terms of timeliness, reliability and scalability(important attributes of the VN).In the next section, we will discuss the novel specifications and technological support provided by edge computing will give pragmatic impact on the security of VN. Furthermore, this new model decreases the requirement of the direct communication in between vehicles at user layer.

III. PRIVACY CHALLENGES IN VEHICULAR NETWORKS

Privacy services are crucial to implement in the VNs because of the existing problems in the road-safety applications. Already available solutions and algorithms mainly focuses on PKI to resolve the authentication[8] issues of the network. Although, this create complexity in data management task, on one hand it requires information sharing while communicating and on the other the shared information can be misinterpreted by the intruder. This work mainly focuses on the research done by various researchers. Every time authentication is performed in VN, it will pass through various phases:

1. ITS initialization phase: This is the first phase in which all participating entities registers themselves using the credentials issued by the ITS certification authority. The main reason is to verify whether the specific node is valid or not. This involves a set of regular edge nodes at every level, RSU and OBU. The issued credentials may have distinct format because of variety of available cryptographic schemes.

2. Communication of entities: V2V and V2I architecture communicate via sending messages to the entities participating in particular system. The complete communication requires the credentials verified during the initialization phase. Thereafter, various cryptographic parameters can be utilized using message authentication codes or signed by digital signatures, de- pending upon the applicable cryptographic scheme. Although, generally we prefer using digital signatures in our message communication.

3. Verification: After a message is received, the vehicles are mandate to check the authenticity and legitimacy of the network used to sent the message. Till this end, it is important to check the information provided by the source is valid or not.

4. Revocation of invalid nodes: This phase revoke those entities having invalid credentials and send report to the upper layer.

As we have explained earlier, realizing authentication and preserving privacy to achieve location privacy is a very challenging task in VANET's. A compromised network node can affects one's privacy and challenge security[9]. A malicious node may spoof the information present in the beacons and misdirect the other nodes. Although, few already proposed schemes challenge to fulfill the both demands in parallel using the very well known approach known as pseudonyms. However, the pseudonyms provide almost equivalent solution as public key cryptography, but pseudonyms cannot be directly link to the original identity of the node. Additionally, to maintain the un-traceability of the nodes, pseudonyms must be change periodically over time or zone changes. It can be achieved by either periodic change of pseudonyms or can be store in a pool of pseudonyms. There is an essential need of revocation authority, to take decisions for misbehaving nodes in VN.

Generally, two approaches have been used frequently for the pseudonym allocation in VN; first approach requires third-party as the trusted body or as decision making body and second method is self-issuance(inclusive 1609.2 standard).This third party may known as central authority(CA), pseudonym provider, registration authority(RA) etc, but the role will re- main same. Apart from these authorities, we have issuance, enrolment, authorization authorities to fulfil the different roles in VN. Till date a number of pseudonym allocation strategies have been

proposed and their categorization can be done on the basis of used cryptographic mechanisms(asymmetric cryptography, identity-based cryptography, group signatures and symmetric cryptography)[10]. Every scheme has their own pros and cons. Out of the given approaches, asymmetric key cryptography and identity-based approaches are voted as the most viable methods for implementing pseudonym in VN. Although, all of mentioned schemes have their own pros and cons (for example, group signatures demands group management of the nodes in P2P model). However, in every case the internal characteristic of every scheme depends on the management of revocation of the nodes credentials. It is essential for the vehicles to verify the message authenticity and credentials used during verification. Considering it as drawback, the responsibility of managing the revocation list becomes the liability of the vehicle nodes itself, which in turn directly impact on the network bandwidth and latency. To avert this overhead, the load can be distributed among the nodes.

There has been few research available on understanding VN digital evidence generation and their custody. In [11], authors have presented a scheme which helps in the reconstructing of accidental events, specially targeting the evidence generation and treatment. Although, how evidence can be collected securely is not covered in their work. In [1] authors introduces the role of witnesses too, to recreate the chain of events of an accident.V2V communication in VN looks promising to enhance the efficacy of road traffic. Yet, it faces many challenges during setup for a communication due to the dynamic nature of the nodes participating in the network. This highly demands additional remedies in order to create safeguards with respect to failures.

Additionally, attacks on availability are considerably most difficult in terms of protection. The well known threat to availability is denial of service (DoS) attacks, a number of false messages is sent by intruder aiming to degrade the functionality of the ITS stations. Since real-time interaction via message is the key of successful VN, methodologies focusing on preventing only ITS stations is essential. Few solution have already been proposed suggesting mainly to change the technologies, channels used for communications or routing topology whenever an attack is suspected. It requires immediate response.

As we have specified earlier, in VN, anonymous certificates or pseudonyms (mentioned in standard 1609.2) have utilized in order to separate the right to access network facilities from drivers original identity. Also, these details must be change after a certain period to remove the chances of traceability and tracking of nodes in VN. Following such rules gives a certain level of anonymity, but in few cases the frequency of pseudonym update becomes really demanding as a drawback of the continuous request of packets from the vehicles. And this request of pseudonym change also carries a cost.

IV. VEHICULAR EDGE COMPUTING

Vehicular Edge Computing(VEC) is combination of mobile edge computing with vehicular networks. There is a misconception about vehicles can be work as edge devices themselves[12].However, vehicles are only end user of our VN model. Few studies shown that the vehicle can work on predictive computation basis by deploying the edge units in the network has been tested[13]. The main reason is that the probability of outsourcing computation facilities, implementation of virtualization provide transparent and while moving tasks completion.

In our work, we anticipate three logically coexisting deployment models of VEC. Our aim is to anticipate these models with less complications than other authors, present the best suitable and real-time scenarios in which they can be compatible with the existing technologies and standards.

1. Deployment models we differentiate among the user and the infrastructure views in the proposed model of VEC. Every view is different from another, as depicted in the fig. The various devices in the infrastructure view are placed in the form of many layers, like in our traditional edge computing models, generally there is a cloud layer and an edge layer. On the basis of edge layer position we can further divide our models into three deployment models:

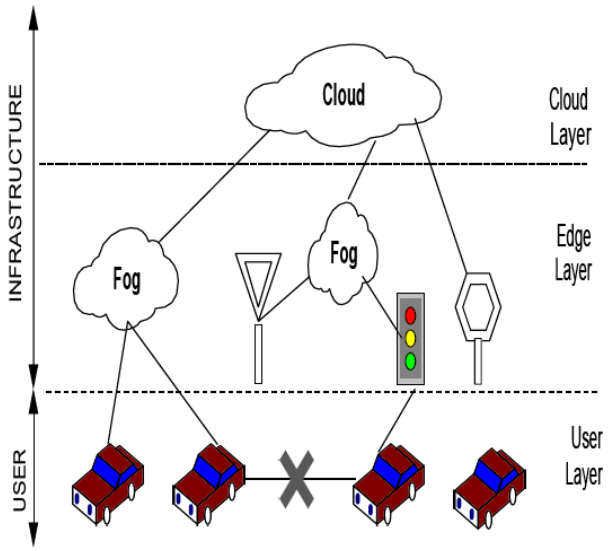

Fig. 2. Vehicular Edge Computing deployment models

a. Fog-based model: This infrastructure is designed on the basis of general-purpose fog devices to paid the VNs. These simple devices have ample storage and faster calculation capabilities through which they are able to manage the complete communication and calculations with the a number of vehicles consecutively, aiding them not only for safety-involving applications but also help in augmented reality scenarios, infotainment applications, analysis of data services, etc.

In general, it is possible in various locations like in urban areas or highways, these devices can be installed in the cellular towers, traffic lights, shopping malls, government buildings, etc. Although, we plan to deploy these devices in sparsely populated regions to mitigate the cost of the

devices. For ex- ample, a number of highways spreads over several kilometers and have almost negligible traffic. In such conditions, this kind of communication models seems unfit and uneconomical, because this demand can be fulfilled by fewer number of wireless devices.

b. Road-Side unit based model: This model involves the use of roadside devices to reinforce the implementation of VNs. These devices are same to the notion of RSU in traditional environment where they are generally synced with the already placed things on the roads such as, road signs, bus stops, traffic lights etc. Such devices commonly have very less storage and calculation capabilities than the edge devices. We can deploy such type of devices in those areas where cellular coverage is low, or jammed. These devices have capability to operate and provide support to the VN without establishing a permanent connection to the higher-layer devices, like cloud. Till now, we have stated that the deployment of this technology is suitable for every place. However, this solution is not efficient in terms of cost when vehicle density is very low and performs better when the density is high, such as in urban areas.

c. Hybrid deployment model: This model is basically involves the best features of other proposed models. The deployment model involves the utilization of dedicated and easily-available edge devices normally arranged in two layers. This is done to provide vehicles desirable communication coverage, additional calculative and memory requirement, and few demands for redundancy. However, this proposed model can be more suitable for the densely populated places. Our belief is that this model is the most promising model in the future of VEC.

In above mentioned model, general-purpose edge devices and RSUs placed on the road are susceptible to be com- promise and hence, security services cannot be taken for granted. Although, it is considered that the installed general- purpose edge devices will be placed into secure facilities and must be furnished with tamper tolerant hardware modules.

An important point to be noted that V2V communication in between vehicle nodes is conquered using such deployment models. Even though, very often used cellular technologies such as C-V2X reinforce the communication in between vehicles directly, but on the other hand it protects vehicles from P2P, collisions and temporary resolution protocols management, following each property transmit upon the infrastructure provided by the edge technology. We must note that, as mentioned that V2V communications are still possible, our study will indicate that privacy can still be enhanced with the amalgamation of V2I communications and edge embedded VNs.

This may be the possibility that overpowering V2V be- yond capacity affects the potential of vehicles to establish the communication among them, even when RSU's are not present. Though, recent developments in cellular communications notably lessen the involved risk. In general, the underlying protocol describes that how vehicles are allowed to establish communication with each other by utilizing the benefits of cellular technology. Nevertheless, there are few regions where cellular signal is not very stable and coverage is also limited. These conditions will not only be comparatively uncommon but tends to occur in areas where the density of traffic is thin, like in rural areas. As mentioned earlier, such condition can be eliminated with the implementation of RSU type devices.

In addition, although the defined communication standards in VN, such as DSRC and WAVE, were not modeled to enfold every aspect mentioned above, they assume the mutual existence with, also the abstraction within, other communication protocols. Hence, the intended deployment models studied can be completed with the already proposed technologies and standards.

V. EDGE-ASSISTED PRIVACY

Few difficulties noticed till now in VN can be mitigated with the righteous application of Edge technology to acclaim privacy features in this scenario.

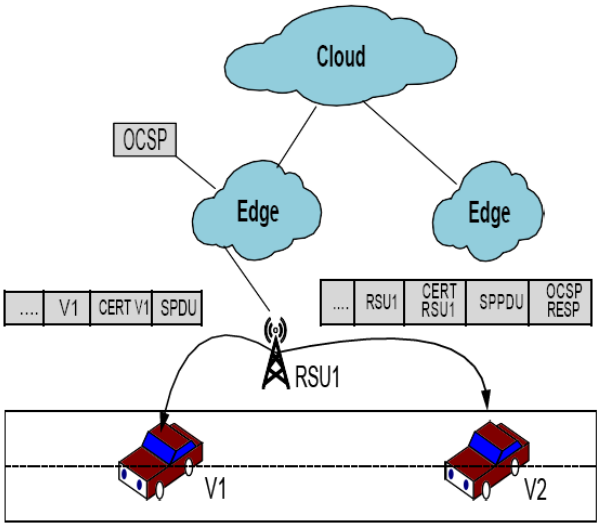

Fig. 3. Vehicular Edge Computing deployment models

As mentioned earlier, another considerable privacy amenities and key to VN is authentication. Although, this does not only helps the amenities in the areas of edge computing. Also consider that the choices are available for the deployment models, but it does not have a important affect on the features analyzed further.

1. Authentication

In conventional VN, pseudonyms and safety-related messages are communicated using either V2V or V2I infrastructure. On the contrary, in our model of VEC, we remove the probability of implementing V2V and accordingly messages communicated by vehicle nodes to connect with other vehicles. The authentication process will remain same as it was performed in VANETs. Hence, a pseudonym mechanism must be present to preserve the identity and location privacy of the vehicular nodes. In order to implement that, methodologies for renewal of pseudonyms are to be

mentioned in this context. As depicted in Fig.3, beacons and safety messages accepted by the edge nodes are updated accordingly to reflect the newly introduced source of the message packet and the information such as GPS data and the source address information to them. This incurs increased cost on edge devices, however the computational overhead forced by packet transformation can be considered as negligible. The most time-consuming task for edge-enabled devices is to validate the status of every vehicle who participates in the network is trustworthy or not.

After confirming the exact status of edge-enabled devices, if it is authenticated the message will be forwarded, receiving vehicles only has to validate the status of pre-installed edge devices. This will definitely decreases the responsibility of CRLs management, because it is not feasible to check the revocation status by vehicle itself.

To understand this briefly, it is assumed that the number of vehicles will be 152M till the end of year 2020.Given the equivalent probability of malicious nodes in X.509 PKIs, it have been evaluated by NIST (National institute of standard and technology) that approximately 10% certificates will be found malicious(needed to be revoked).In conclusion, 15.2 million revoked certificates will be available in the CRLs. An standard X.509 certificate size is 27Mbits, represent that generally a short-range connection will require 9 seconds to download the complete CRL, which is crucial time for decision making in safety-applications.

The VEC is of distributed nature which does help overcome the above mentioned issue. It is also feasible to keep the whole CRLs in the cloud and present only requested part to the specific vehicle at some geographical location. Then after, these part of CRLs are managed by a surrogate certification authority present in reliable edge devices. The distribution of such services among the VEC infrastructure also helps in finding the malicious nodes in a more timely manner. The noticed alterations can be update at a later stage. This improves the response time of the network and time-sensitive operations can be done in real time.

2. Anonymity

The introduction of edge technology into the VN provides few additional privacy features. Transmission of data from one vehicle to another via edge enabled devices abstracts the source vehicle identity and therefore the sender has capability to safeguard its pseudonyms, because, for a particular time, the communicated beacon message can be re-transmitted by the edge-enabled RSU node. For example, there is an accident occur on the road and a number of vehicles are involved, the closest vehicle quickly reports the alert message to the nearly-placed Edge. By receiving the edge node act accordingly, this is a simple scenario depicting comparatively less number of pseudonym exchange is needed.

Another advantage is on the data analysis work can be done by the infrastructure. As the data travels towards the upwards direction the data is aggregated and context-aware services are furnished to expands the geographical positions. Hence, if any upper layer becomes compromised by an intruder, the data stored does not contain recognizable information and its privacy can be at risk. To overcome such problems, a fog-driven traffic model is suggested, which is capable to make local and global decisions separately for traffic signals[14]. These global decision making involves the aggregated stored data to keep the drivers private.

Thanks to the use of inherent secure virtualization and SDN (Software Defined Networks) in Edge Computing technologies, the need of computing power and storage requirements can be predicted [15] and distributed as needed.

3. Analyses of digital evidence and detection of malicious nodes

The most important point is that both edge and vehicle nodes are susceptible to be compromised. After receiving the message receiver cannot affirms that the message is authentic or not and unable to recognize the actual malicious intended entity in the network. Such forged message may be received from the network or from the direct vehicle itself, because both possibilities are present. This problem can be mitigated if the edge nodes keep the record of received messages. However, this will increase the overhead of the network. For example, a vehicle who is sending falsifying information about the condition of the roads can be identified by the VEC infrastructure, then appropriate actions like revocation of certificate and reporting to the authorities will be done later.

Therefore, whenever a message is received by a edge node from a vehicle, it requires categorization. Safety-assisted messages falls into higher priority category and for other category of messages, no record will be stored. The upper layers are updated with the stored data after a period of time. Hence, RSUs and edge nodes are require to store the data for a very short time.

Whenever the stored data is transmitted to the upper layers, a data analysis task is done by an intermediary edge node to find out the malicious nodes or falsifying communications. Since this work does not require the involvement of cloud server itself, this helps in pointing out the possibility of attacks with respect to the location of the vehicles.

The higher layers in the model has more powerful methods to analyse functions. For example, assume if a pseudonym x used to communicate at a particular location and again same pseudonym is used to communicate at a remote location, assuming 50 kms far from the previous location, intermediary edge nodes are capable to head-on revoke the certificate credentials of that node. Additional example of such problem is mention in [14], introducing big data analysis to detect the malicious nodes in the VN.

VI. CONCLUSION

Edge technologies are considered to be the remodeling technology for the vehicular networks, as it modifies the method of interaction among devices and the vehicles. This technology has become the integral part of the vehicular networks by providing the features such as complete digital devices with sensing, computational and communication capabilities.

In the imminent future, we will foresee our vehicles are equipped with some fascinating features such as, highly mobile, real-time, focusing on safety, security and privacy applications. Besides, as important components of the intelligent transportation system analytical infrastructure, if any attack occurs it will not only disturb the network but may hamper the human lives. This is the fundamental reason of this research work, it bridges the edge technologies with mandatory features like authentication, anonymity and analyses of available digital evidences. Our believe is that edge technologies will be thoroughly introduced to enhance the privacy services by managing the global and local locations and computation of cloud servers in the vehicular networks.

REFERENCES

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Iban˜ez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[2] R. Al-ani, B. Zhou, Q. Shi, and A. Sagheer, "A survey on secure safety applications in vanet," in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 1485–1490, IEEE, 2018.

[3] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[5] F. Zidani, F. Semchedine, and M. Ayaida, "Estimation of neighbors position privacy scheme with an adaptive beaconing approach for lo- cation privacy in vanets," *Computers & Electrical Engineering*, vol. 71, pp. 359–371, 2018.

[6] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pp. 19–28, ACM, 2007.

[7] J. A. Onieva, R. Rios, R. Roman, and J. Lopez, "Edge-assisted vehicular networks security," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8038–8045, 2019.

[8] Z. Yan, P. Wang, and W. Feng, "A novel scheme of anonymous authentication on trust in pervasive social networking," *Information Sciences*, vol. 445, pp. 79–96, 2018.

[9] M. Gupta and N. S. Chaudhari, "Anonymous roaming authentication protocol for wireless network with backward unlinkability and natural revocation," *Annals of Telecommunications*, pp. 1–10, 2018.

[10] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228–255, 2014.

[11] A. Wasef, Y. Jiang, and X. Shen, "Dcs: an efficient distributed-certificate- service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 533–549, 2009.

[12] Y. Xiao and C. Zhu, "Vehicular fog computing: Vision and challenges," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 6–9, IEEE, 2017.

[13] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 36–44, 2017.

[14] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: architecture, use case, and security and forensic challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, 2017.

[15] A. Ermagun and D. Levinson, "Spatiotemporal traffic forecasting: review and proposed directions," *Transport Reviews*, vol. 38, no. 6, pp. 786– 814, 2018.