I.J. Modern Education and Computer Science, **2019, 1, 39-44**
Published Online January 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2019.01.05

Efficient Authentication and Privacy Mechanism to protect legitimate Vehicles in IEEE 802.11p Standard

Deepak Verma
M.tech (IT) student Chandigarh Engineering College Landran (Mohali)
Email: deepakverma717@gmail.com

Dr. Parminder Singh
Associate Professor Chandigarh Engineering College Landran (Mohali)
Email: singh.parminder06@gmail.com

Received: 08 October 2018; Accepted: 27 October 2018; Published: 08 January 2019

***Abstract*—**VANETs is the open model which stimulate in academia and industry oriented researches. However, the model is open and there are many violations in a communication of vehicle to vehicle (V2V) and Vehicle to Infrastructure (V2I). Any anonymous user may extract the useful information. Researchers have proposed many research proposal and solved issues related to VANET. The security is the major concern and to avoid mishappening in driving the vehicle. We proposed the authentication system that provides safety of the driver during travel on the roads. The proposed results deliver the following features: 1) Reliability of VANET model 2) Road Safety 3) Privacy of the vehicles 4) Authentication of message delivery to adjacent nodes. Finally, we provide a view point of how to detect the attacks and withdraw malicious node more efficiently.

***Index Terms*—**VANET, V2V, V2I, RSU,MAC, OBU.

I. Introduction

For Smart transport system, Vehicular Adhoc network is the solution to avoid road accidents and traffic congestions. There are number of user applications flow in vehicle to vehicle and vehicle to infrastructure in VANETs [1] . The messages which could be flow in transmission like warning messages, route diversion message and emergency event happen [1]. However, the emergency event messages can be observe under the controller so that the message should be sent to right user. VANETs have the potential to transmute the messages to the handlersthrough interoperable wireless channels [2]. These wireless channel has operated on the IEEE 802.11n standard and IEEE 802.11p functioning on the VANETs. The two standards have different data rates and transmission ranges but we implemented these two different standard in the proposed scenario. The IEEE 802.11n and IEEE 802.11p are different standards which is named as heterogeneous system and the heterogeneity generally equipped with number of components of the VANETs. The components of the VANETs are Road Side Unit (RSU), Integrated Circuits, Intelligent control which has capability to operate on wireless systems.

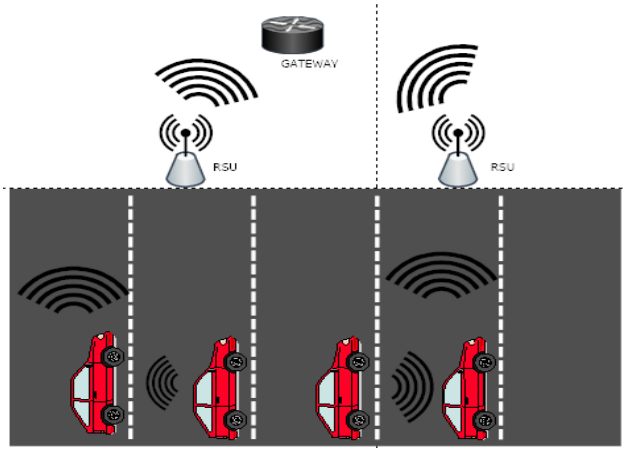

Fig.1. VANETs Architectural Model

Automobile industry have started the safety measures to the customers and deploying safety enhancement equipment's in the vehicle [3].These hi-tech equipment's incorporate safety measures in all aspects, comfort of traveling and passengers entertainment. The RSU unit preserved like a wireless Access point though sending beacon information to Gateway. The problem of the current scenario, illustrated in figure 1, is that any adversary node listen the communication (Stream socket) in the path and inject some bogus messages to block the communication in the path. The resultant output will be horrible, the messages is not sent to the proper user. This is the critical problem in smart transport because every smart vehicle link to some IoT device and the IoT devices connected to the wireless Access points. Access points is liable for forwarding the data to Gateway. The main problem of the current transport system is

Authentication. The authentication in the transport system means that every single vehiclegive all the details related for identification proof to the Access point. The Access point has designated a duty to store the MAC address of the Vehicular machine. The MAC address and other related information like protocol used, IP address, Connection time (Establishment, Connected and Terminated) will be stored on the web server. Now, the web server delivers the information to the driver of the vehicle in the form of Text. The security related problems has been solved in this paper through Authentication based mechanism. If the messages will be delivering in the excessive manner then we apply the flow control mechanism. The flow control mechanism has been referring to the RFC of Transmission control Protocol (TCP). The verification process in the smart transport system has been solved by storing the MAC address in to the Gateway of the corresponding RSU of the vehicle. To improve the verification efficiency, the RSU unit receive the new MAC address of the newly vehicle and only give accessibility to the vehicle when allowed by the Gateway.We are implementing three security mechanism system in our proposed system i.e. Authentication, Privacy and Confidentiality.

The contribution of this paper can be addressed as following manner:

1. The privacy mechanism to conduct comprehensive assessment of messages, operations and privacy to overall network.
2. The Authentication mechanism is focus on this paper for identifying the potential of message dissemination, as protection of driver's safety.
3. The flow control of the system is taken care in the paper so thatanonymous user will not send numerous messages to the driver. Brute force attack (source machine send number of messages to the destination machine) has been stopped by the proposed mechanism.
4. Employing Hypothesis model to perform mathematical operations to handle encryption and decryption tasks.

A. Background of the VANET Network

Basically, the reference model (depicted in figure 2) of the VANET has operated on the Physical Layer, Data link Layer, Network Layer, Transport Layer and Application Layer. The Application Layer responsible for User Application related services including people and business processes. The Layer collaborated with multiple applications and generate emergency events, location and velocity. Data in motion is converted into data at Network Layer. The data is suppressed for high level processing. The routing protocols has used to support different communication paradigms illustrated in Figure 3. The main goal of this communication paradigm is to provide the data to destination users. In our paper, we are using Mobile Control Transport Protocol (MCTP) is based on the same principle of Transmission control protocol. The advantage of this protocol is to handle web based applications. In paper [4] classifies the HTTP (Hyper Text Transfer Protocol) related attacks on the port number 80. The behavior of attack is different from one another, therefore, each attack to be identified through MCTP. The performance of the network is also measured through Training set of data, is collected from Network Simulator (NS-2). The TCP protocol is the superset of HTTP protocol so to identify the attack on the transport layer is easily identified.

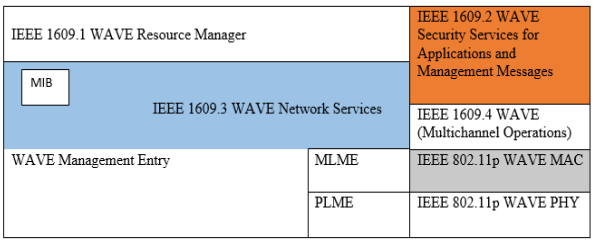

Fig.2.VANETs Reference Model[5]

Vehicle to vehicle transmission definitely end at Physical layer. The bits are usually transmitted through Radio and Infrared waves. Both these waves are suitable line of sight communication. In our experimental model, we assume that a radio channel for transmitting vehicle A to receiving node B is established if and only if the power of the radio signal at Road Side Unit C is above a threshold. Suppose if the power is suitable and reasonably good communication among the nodes then we fix the threshold value P (A, B) and this power P could be fixed in throughout the network. Dedicated Short-Range Communication (DSRC) system in VANET is a short to medium range communication that operated at 5.9 GHz band. DSRC system supports vehicle speed up to 200 km/h and this vehicular speed hold the transmission range up to 300 meter. This transmission range extended up to 1000meter and the default rate is 6Mbps. IEEE 802.11p based on earlier standard of IEEE 802.11which is a wireless standard and gives a speed up to 2Mbps. IEEE 802.11p controlled the MAC layer and focus is to reduce the collision.

The rest of this paper is organized as follows. In section II, Related work on VANET Security and misbehaving the Vehicles is reviewed. Section III, We describe the research problems in detail. In section IV give the description of the proposed framework. Section V will be finding the performance of the proposed system and compare with existing system. Finally, in Section VI, summarized the paper.

II. Related Work

Several Security models has suggested in VANETs as well as trust models of AdHoc Networks.Privacy and Authentication is the main priorityof the AdHoc System.Many researchers contribute on this modelto prioritize the security in between V2V and V2I Model[2][3].The proposed authentication system [6] is based on cryptographic protocol that issued the challenge to the Vehicular nodes who being communicate in the

AdHoc networks. Before the verification process has completed by the main node, the private and public key provides confidentiality. The set of public keys and private keys has stored on the undirected graph G= (V, E). Another proposal proposed by the Authors [7] that explain the performance degradation of the system during lack of security. The Authors employ the Ant Colony Optimization techniques to compute the feasibility of the routes in Vehicular AdHoc Networks. Each vehicle shows a unique identity C_v over the network and the certificate CA issued to the trusted vehicles. The public key of the CA as generate the hash value of the agreeing data. The vehicles could not disclose their location to strange vehicles before the proposed system deploy on the Base Station. Another possibility of the attack is the Open Air Communication [8], therefore, Security and the privacy are the main concern of Vehicular Model. The First Step of the proposed System to identify information like home address and Identification number. After the First Step, the next process is to assign the private and public key pairs along with vehicle certification. The whole process handle by the Road Side Unit (RSU) which helps to authenticatethe integrity of the message. Authors [9] describes the project that integrate smartphone and IEEE 802.11p standard. The novel idea of this paper has provide Smart Drive facility to the customers. The onboard unit has placed inside the vehicle and communicate to RSU unit which is deploy on the road intersections. The number of problems faced by the customers are traffic collision, and road safety. These problems are avoided by the proposed VANET based system that can provide a reporting facility. The SMaRTDRIVE application can report about the road accidents, traffic Jam and hazards. The new system [10] based on trust based management system incorporates to enhance the security level of the Vehicular AdHoc Networks. The proposed schema has cut down the false warning messages to the cluster founded vehicular networks. Operated frequency is 5.9 GHz that covers the distance up to 1 Kilometer. The application designed for this model is to grow the communication of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I).Authors [11] believed that information only exchanged through onboard units and each vehicles on the network is requested mode. The aim of the paper is to provide better services over the Internet. It was figure out that authentication based communication only conceivable through session keys. These session keys overwhelmed the security issues during establishment of the connection between OBU and RSU. The session key based approach implemented Elliptic Curve Cryptography (ECC) and these are distributed among the scenario via message broadcast. Another new concept [12]was came to light is Internet of Vehicles (IoV).This concept used the data set of 2.3 million injuries and conclude that it was occurred due to lack of road conditions and traffic congestion. Every vehicle had contact to the internet and we need a security of the network. It is possible to protect the network of such data manipulation attacks. The source node sends the hash value information to the receiving node. Receiving machines runs the same algorithm against the hash value of the source node. If the value does not matches then vehicle tear down the connection. The objective of the paper [13] is to completely avoid the Denial of Service (DoS) attacks. These type of attacks addressed by the proposed multi-layered game theory framework and volume of traffic has minimized by modeling the interaction of IDS based System. Firstly, the author made clustering based algorithm that enhanced the performance of the clustering. The prioritized packet who have communicate earlier give the advantage to communicate during data routing. Secondly, Game theory based network identify the attack signatures through IDS System.

III. Research Problems

Kang et al., 2016 created a new Intrusion Detection Based System which is authenticate the message in vehicular networks. The whole system has worked on batch verification mechanism which ensure the confidentiality of the system. The recovery of lost messages were also explained in the message authentication based system. The proposed system models were contains three parts such as trusted center, roadside unit and onboard unit. These parts associated in running vehicle and care about accident scenario[1]. The probem of the system is to depend on the speed capabilities but we observe some frequency mismatch in the model so we can carry on the work in our proposed model.

Hasrouny et al., 2017 has focused on various threats that havepenetrate the vehicular system and these threats is the matter of the concern. Some of threats posting the scripts on the wireless interface and track the messages. This type of attack reflects the Denial of Service (DoS) type attack that trying to make services unavailable to the driver. This attacks is very dangerous in the safety point of view. Other related wireless interface attacks are Sybil attack, Man In The Middle (MIM) attack, Brute Force attack and Black Hole Attack. Another type of attack that potentially happened on the Device Firmware and Software System of the vehicle. Message Alteration and Broadcast Tampering are possibilities of this Threat. Public Key Infrastructure (PKI) is the option to defend these types of attack[14] but given model not detected under any technology.

The following issues **(Subba, Biswas and Karmakar, 2018)** of the IDS System has considered in the system that to adopt clustering algorithm for dynamic network topology. The topology may cause higher delays due to broadcast storm at high density rates of the vehicle. There were two lists maintained for detection of attacks, Malicious List and another is suspicious list[13].

Sattar et al., 2018 assumed that broadcast scheme is the one factor to dominate the reliability of the network. If multi-hop VANET and end to end communication possible on the experimental testbeds then it improves the

performance of the network. The communication possible at Network Layer and theoretical results examined through simulations. CSMA/CA protocol enters in the back off mode that find the state of the channel[15].

Li et al., 2018 suggested the feasible solutions of vehicle safety. Thus, the researchers launch the attack through Controlled Area Network (CAN) bus. It shows that how the attacker exploit the vehicle and gain access via wi-fi. Brute force attack and key fob algorithms may crack the password. Another possible attack is firmware attack that is possible through CAN protocol. Suggested technique are cryptographic and IDS based system hat obtain the type of attack and mitigate those attacks[16]. These attacks generally very time consuming and result are not optimistic.

IV. Proposed Framework

The conventional method has not solve the Authentication process because if the Asymmetric Algorithm is used on the system then the whole network is very complex to maintain the two-key process. The two key process need more speed and required large data space to maintain the data. The following assumptions has been used in this paper to implement theoretical model and this model will implemented through Network Simulator.

Case 1: (Cluster equivalence)

Let's assume there is N network which belong to three different clusters ç1, ç2 and ç3.

$$ç1(\ldots\ldots - x3, -x2, -x1, x0, x1, x2, x3\ldots..) \quad (1)$$

$$ç2(\ldots\ldots, -y3, -y2, -y1, y0, y1, y2, y3....) \quad (2)$$

$$ç3(\ldots\ldots., -z3, -z2, -z1, z0, z1, z2, z3\ldots\ldots.) \quad (3)$$

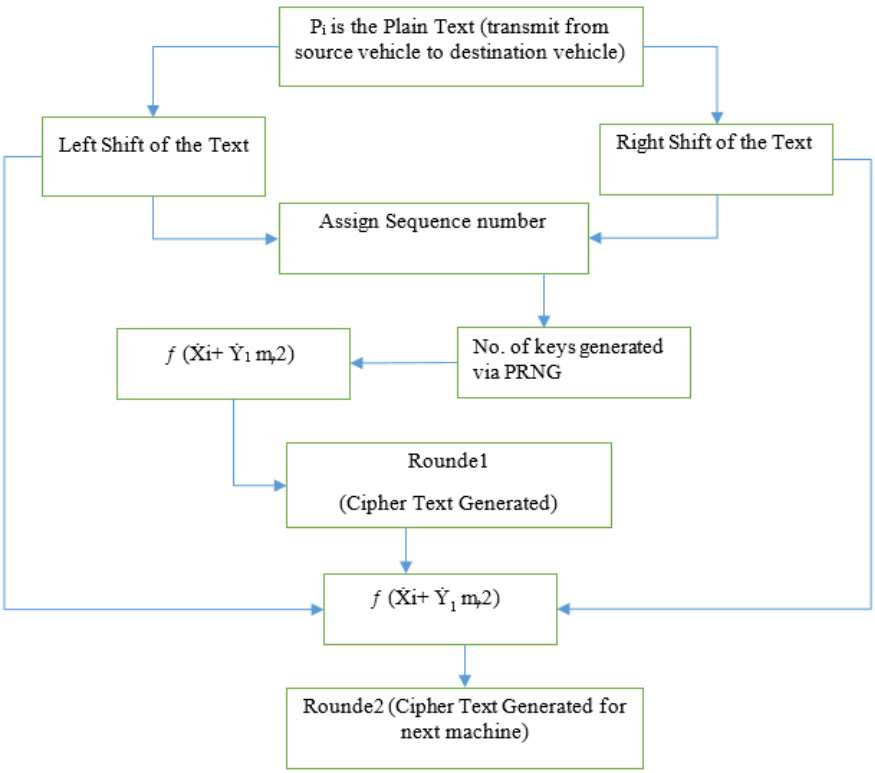

Fig.3. Flowchart of Challenge Assumption

Suppose there are different variables which belong to the clusters and these are equipped with one group $Ğ_1$. Similarly, efficient computable of IEEE 802.11p, $Ğ_1$ ϵ integer values. The output of the parameter depends on modulus operation. The definition of the modulus operator is [15]:

Let a, ŦŦ, m ε $\mathbb{Z}$ and m>0 {that means the value of modulus is always positive integer}

We write,

$$a \equiv \check{T} \ mod \ m \left\{ the \ value \ of \ a \ is \ equivalent \ to \ \check{T} \right\}$$

If m divides $\left(a - \check{T}\right)$ *then* If m divides (a-ŦŦ) then

$$m \left| \left(a - \check{T}\right) \right. \quad (4)$$

Case 2: Cluster to Cluster Communication

Suppose the different set of clusters want to communicate to each other and we are applying the equation (1). This equation apply only when the authenticity provided by the cluster head of each cluster (Ç1 X Ç2).

$$A = \left\{\mathbf{x_0}, \mathbf{y_0}\right\} \tag{5}$$

The new group A get the value of two groups of cluster i.e. $\mathbf{x_0}, \mathbf{y_0}$.

Now, if we apply the equation 4,

$$\begin{aligned} & m \mid \left(a - \check{\mathrm{T}}\right) \text{ then,} \\ & a = \mathbf{x_0}, \check{\mathrm{T}} = \mathbf{y_0} \\ & m \mid \left(\mathbf{x_0} - \mathbf{y_0}\right) \end{aligned} \tag{6}$$

Above Assumptions, It was cleared that the cluster behave equivalent only when the modulus is same and the output value of the A is zero.

V. Results and Discussion

In the VANET model there are more than one cluster in the network and connected in Ç1, Ç2 and Ç3 groups.Each cluster group connected to different path and vehicle travelthrough multi-paths. An important observation has beenillustrating in figure 4 which gives the throughput of the network.In particular, our network it is very difficult to analyse the value of the throughput because the paths are disjoint and nodes are moving with speed at 20Km/h.In meantime, the proposed model also provides authentication of the system. The maximum throughput in our result is 80 Mbps which is higher than existing approaches [17]and it is assumed that the ratio of the packet loss is minimum our case becausethroughput is directly proposional to the PDR.

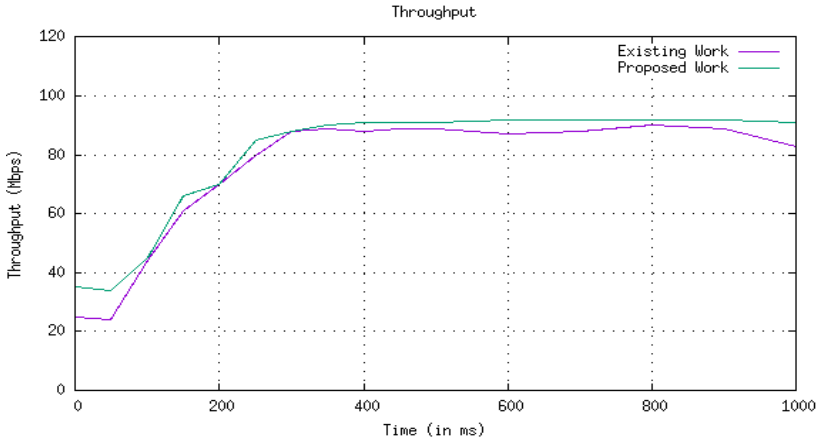

Fig.4. Throughput comparison of Proposed and Existing work

Figure 5 illustrates the PDR versus different size of the network. In the existing work[15], the PDR is less due to interference but the proposed model provides higher throughput and the value of PDR also improved. The network size expanded exponentially and therefore, the PDR value never decreases because the process of the proposed model is light weighted and flexible to the VANET environment.

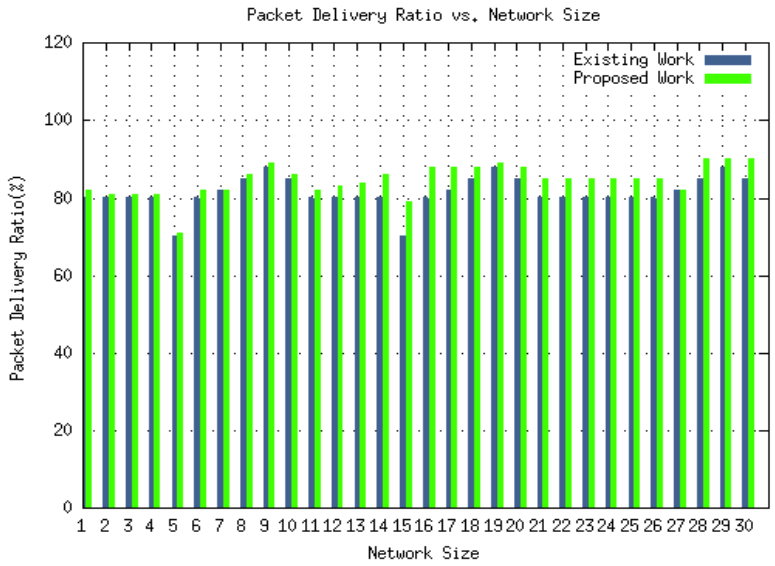

Fig.5. PDR vs. Network Size comparison of Proposed and Existing work

VI. Conclusion and Future Work

We have presented the architecture of VANETs that give the idea about the working of the vehicle on the road. The different component of the vehicle like RSU, OBU functioning like an IEEE 802.11p standard. These components executed in different communication standards such as vehicle to vehicle (V2V) and Vehicle to Infrastructure (V2I). Though security of the VANET is the major concern and the process has been solved for further proposed Authentication model. However, the model ensures the privacy concern in the network and detect legitimate vehicle that have a chance to become a malicious node. The proposed model gives packed resilient security against these malicious adversaries' nodes. The future work to take up in IoT related model and the IoT hybrid model allied to 5G networks.

References

[1] Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li, "Efficient authentication and access control of message dissemination over vehicular ad hoc network," *Neurocomputing*, vol. 181, pp. 132–138, 2016.

[2] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, 2016.

[3] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs," *J. Netw. Comput. Appl.*, vol. 36, no. 5, pp. 1352–1364, 2013.

[4] M. M. Abd-eldayem, "ORIGINAL ARTICLE A proposed HTTP service based IDS," *Egypt. Informatics J.*, vol. 15, no. 1, pp. 13–24, 2014.

[5] F. Cunha *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016.

[6] C. Caballero-Gil, P. Caballero-Gil, and J. Molina-Gil, "Mutual authentication in self-organized VANETs," *Comput. Stand. Interfaces*, vol. 36, no. 4, pp. 704–710, 2014.

[7] M. H. Eiza, T. Owens, Q. Ni, and S. Member, "Secure and Robust Multi - Constrained QoS aware Routing Algorithm for VANETs," *IEEE Trans. Dependable Sec. Comput.*, vol. 13, no. 1, pp. 1–14, 2014.

[8] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, 2015.

[9] P. A. Sumayya and P. S. Shefeena, "VANET Based Vehicle Tracking Module for Safe and Efficient Road Transportation System," *Procedia - Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 1173–1180, 2015.

[10] A. Ltifi, A. Zouinkhi, and M. S. Bouhlel, "Trust-based Scheme for Alert Spreading in VANET," *Procedia Comput. Sci.*, vol. 73, no. Awict, pp. 282–289, 2015.

[11] R. Muthumeenakshi, T. R. Reshmi, and K. Murugan, "Extended 3PAKE authentication scheme for value-added services in VANETs," *Comput. Electr. Eng.*, vol. 59, pp. 27–38, 2017.

[12] D. B. Rawat, M. Garuba, L. Chen, and Q. Yang, "On the security of information dissemination in the Internet-of-Vehicles," *Tsinghua Sci. Technol.*, vol. 22, no. 4, pp. 437–445, 2017.

[13] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 12–28, 2018.

[14] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, 2017.

[15] S. Sattar, H. Khaliq, M. Saleem, S. Mumtaz, and J. Rodriguez, "Reliability and energy-e ffi ciency analysis of safety message broadcast in VANETs," *Comput. Commun.*, vol. 119, no. June 2017, pp. 118–126, 2018.

[16] X. Li, Y. Yu, G. Sun, and K. Chen, "SECURITY AND PRIVACY OF CONNECTED VEHICULAR CLOUD Connected Vehicles ' Security from the Perspective of the In-Vehicle Network," no. June, pp. 58–63, 2018.

[17] R. Kolandaisamy *et al.*, "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks," vol. 2018, 2018.

Authors' Profiles

Deepak Verma, is currently pursuing Master of Technology (M. Tech) in Information Technology from Punjab Technical University, Jalandhar. She had completed her B.Tech in Information Technology from Lovely Professional University,Phagwara in 2009.

Dr.Parminder Singh is a young dynamic personality with a proven record of a good academician and researcher having an outstanding academic record. He has been working as an Associate Professor in Information Technology Department and has more than Ten years of rich experience as an academician and researcher. He has published over 70 Journal and conference papers in the areas of Networking, Wireless Networks, sensor computing and Network security. He has also contributed various articles published in Elsevier Book and Springer Berlin Heidelberg. He has won best-paper awards including the IEEE "Best Paper Award" in the Year 2012 and 2014. He has served/serving in International conferences as a general pc co-chair, and steering committee member, and presented Expert Lectures in the areas Wireless Networks and sensor computing. He has received faculty excellence and research awards in the year 2011, 2013 and 2015 from his Institution for excellence in research, teaching and service.

How to cite this paper: Deepak Verma, Parminder Singh, "Efficient Authentication and Privacy Mechanism to protect legitimate Vehicles in IEEE 802.11p Standard", International Journal of Modern Education and Computer Science(IJMECS), Vol.11, No.1, pp. 39-44, 2019.DOI: 10.5815/ijmecs.2019.01.05

