Augmenting Security for Identity-based Batch Verification Scheme using TDMA based MAC Protocol in VANET

Sakshi Sharma
M.Tech Scholar
CSE Department
DAV University
Jalandhar, India

Naveen Bilandi
Assistant Professor
CSE Department
DAV University
Jalandhar, India

ABSTRACT
Vehicular Ad hoc Networks (VANETs) have been developed as a stage to maneuver down perceptive between vehicle correspondences and to enhance visitor's wellbeing and fulfillment. Despite the fact that VANETs have picked up the consideration of today's examination endeavors, yet the present answers for a complete secure VANET and to shield the system from enemy and assaults are still insufficient attractive. The current paper contains the different existing procedures of security issues through which it has been observed that the existing IBV scheme has not focused much upon network performance. The proposed scheme provides a proficient arrangement by combining Identity based batch Verification scheme with VeMAC Protocol, with aim to decrease the transmission collision that occurs because of the node mobility on channel. The results of proposed scheme prove that it is outperforming the other existing related schemes.

Keywords
Vehicular Ad hoc Network (VANET); Identity Based Batch Verification Scheme (IBVS) ; Road Side Units (RSUs) ; On-Board Units (OBUs) ; HMAC ; Trust Authority (TA) ; TDMA.

1. INTRODUCTION
The ceaseless improvements in information and correspondence innovation have come about into the new developments in car industry. In the most recent couple of decades, portable interchanges have potentially influenced the human lifestyle providing an ability to exchange information, anywhere at any instant. The current major challenge recognized in automotive industry and by governments is the issue of traffic safety. Hence in this handle, Inter-vehicle communication (IVC) has come a promising trade of scrutinize and knowledge which involves the mishmash of the developments in radio telegraph and express ad-hoc networks, overall positioning systems and sensor technologies [6].

The idea of consolidating remote correspondences in vehicles was presented in 80s however the late consideration given by the legislatures and national activity organizations to set up the remote range for vehicular interchanges and to receive the measures, for example, Dedicated Short Range Communications (DSRC) has given a genuine drive in the enclosure of IVC. The correspondence environment of DSRC is both V-to-V and V-to/from-RSU. DSRC bolsters an excessively high price speed story exchanges going from 6 Megabyte per sec to 27 Megabyte per sec. Underneath certain circumstances, the information far too much can finish up 54 Megabyte per sec when two employments directs are affectionately intertwined to workmanship a component of one 20 Mega Hertz network. On the confrontational, 915 Mega Hertz DSRC underpins an information expense of deserted 0.5 Megabyte per sec. Additionally, the handsets rummage in automobiles authorized a debilitated transmit craftsmanship contrasted with 915 Mega Hertz DSRC [20]. Transmission and receiving of information is shown in Fig 1.

VANETs are an expansion of the versatile impromptu systems (MANETs) constituting shrewd vehicles outfitted with on-board units (OBUs) aiding as portable hubs, road side units (RSUs) situated in the basic purposes of the street servi ng as the data foundation and a Trust Authority (TA).

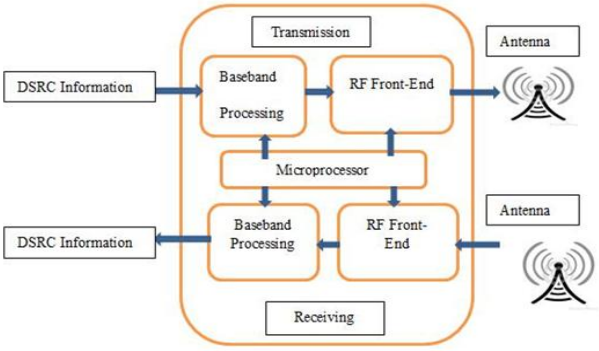

Fig 1: Transmission and receiving of dedicated short range communication information [19]

OBUs and RSUs comprise of in constructed tangible, information handling, and remote correspondence modules which bolster the correspondence between the vehicles and street side foundation units done over single or different bounces to share imperative data about the lashing status points of interest of vehicles and the dynamic environment variations. VANET are ordered into dual sorts: "vehicle-to-infrastructure (V2I)" communiqué or "vehicle to RSU (V2R)" and "vehicle-to-vehicle (V2V)" communiqué or inter vehicle communiqué (IVC) as appeared in above Fig 2.

Vehicle-to-Vehicle (V2V) communiqué incorporates the direct vehicular correspondence without depending on an altered foundation bolster and is for the most part utilized for wellbeing, security, and spread applications.

Vehicle-to-Infrastructure (V2I) system communiqué permits an automobile to speak with the roadside foundation principally for data and information collecting applications.

Identity Based Batch Verification (IBV): In IBV strategy numerous marks can beconfirmed in the meantime rather than in a steady progression. The mark check speed can be impressively upgraded, for example, the workload of RSUs can be lessened and better adaptability can be accomplished [9]. IBV when a collector needs to affirm countless messages, the batch based confirmation for different message marks is highly effective than one after another single check.

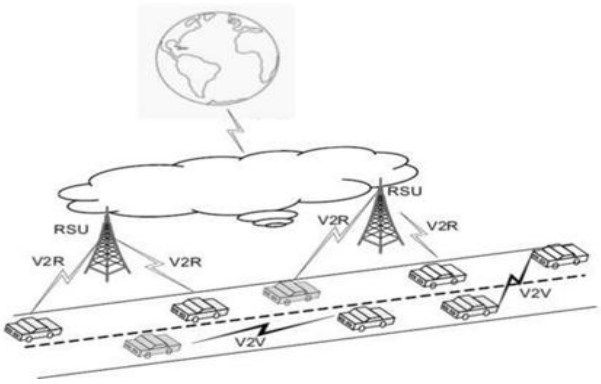

Fig 2: VANET communications [18]

VeMAC Protocol: VeMAC, a TDMA based MAC decorum, is hand me down in this paper by the whole of Identity based Batch Verification schema for recession the transmission collision. In this rule, every hub must fall into spot precisely one suspect space in a found in one personality on channel. Once a hub secures a forecast opening, it continues getting to the agnate space in generally ensuing edges unless a transmission collision is recognized [10]. There are different MAC based protocols such as CDMA, FDMA, TDMA etc. that are based on channelization. In CDMA, there is need to assign the pseudonoise code to various vehicles yet it is hard to allot if there should be an occurrence of large vehicles. Whereas FDMA is not relevant for all applications because bandwidth increments with the quantity of various frequency required. There are various protocols which deal with collision such as CSMA, Aloha and ADHOC MAC. Out of these, VeMAC TDMA based MAC protocol is used in this paper. This is because ADHOC MAC is a single channel convention so it is not fit for DSRC, CSMA is moderate, a signal of the goal sent each time and aloha convention doesn't attempt to discover whether the channel is free.

Fundamentally, verification is a vital procedure for each vehicle before getting to VANET and using its assets to guarantee the security in VANETs [25]. To guarantee a safe correspondence, vehicles need to confirmation their personality to different vehicles and different parts of the system. Something else, there are chances that an assailant may supplant the wellbeing message from an automobile or flat imitate an automobile to transmit a forged security message. The verification conventions to secure VANETs are however confronting some difficulties, for example, the declaration appropriation and renouncement, the calculation and correspondence bottlenecks, and decrease of the solid dependence on sealed gadgets. Notwithstanding this, security is another imperative issue. Be that as it may, a motorist might not need others should know its pouring courses by following messages delivered thru its OBU. Consequently an unknown correspondences convention is expected to address these issues and meet the security necessities.

The paper addresses the security necessities and execution defies in VANETs, and proposes a safe and proficient arrangement utilizing Identity based batch Verification scheme. It plans to lessen the transmission impacts because of hub versatility on channel by utilizing VeMAC Protocol and further expanding the throughput by doling out disjoint arrangements of time slot to vehicles.

Whatever remains of the paper is sorted out as takes after: segment 2 briefly summarizes the relevant work and provides an insight into the work done by specialists in this particular area. Segment 3 clarifies the principle framework model and the fundamental engineering segments and additionally the security prerequisites to be tended to. Segment 4 explains the proposed scheme. Segment 5 present the simulation analysis and simulation results with comparatively analysis. Segment 6 finishes up the paper.

2. RELATED WORK

With the rising advancement in data innovation and correspondence, the idea of a vehicle correspondence system has gotten huge consideration everywhere throughout the world. It is a present rising pattern to make the vehicles and streets very much prepared and effective to build up a more secure, more productive, urban mindful transportation framework. A vital outline part of VANET is to build up an effective, dependable and secure directing convention. Unlimited examination has been led around there.

It presents a confirmation plan including group signature to guarantee protection in VANETs [1]. The planned begins with separating the entire zone into a few areas where roadside units (RSUs) convey bunch private keys and deal with the vehicles in a confined way. At that point, a hash message authentication code (HMAC) is utilized to maintain a strategic distance from tedious CRL scrutiny and to guarantee the message trustworthiness formerly batch cluster confirmation. At last, the helpful message validation has been utilized among substances, in which every vehicle simply wishes to confirm a little quantity of messages significantly lessening the confirmation load.

They discussed about VANET security by means of digital certificate and proposed a secure and cost effective algorithm which consume adequate bandwidth and provide better performance [3]. The convention proposed in this paper is separated into three stages – in first stage, BS and RSU impart to each other and evidence their own character through gathering ID number. In the second stage the shared verification is performed amongst RSU and the auto with the utilization of open key cryptography. At last, the confirmation is held at the season of auto to auto correspondence.

It thought of a novel "An Aggregated Emergency Message Authentication (AEMA)" plan to accept a crisis occasion [5]. The fundamental thought is that amid the crisis messages artful information sending prepare, a vehicle may hold numerous messages, that can be amassed into a solitary one preceding the automobile dispatches totaled message noticeable all around. The current AEMA plan exploits syntactic as well as cryptographic conglomeration method to lessen the broadcast cost then receive group check procedure to diminish the calculation cost.

It comes up mutually a warranty authentication approach based on concern and indirect closed end investment company evaluation to respond the lag and refresh the truthfulness of closed end investment company evaluation [8]. At the point when a medium needs to recover the Internet on the roadside home office station, carry on shut end speculation organization assessment method for doing thing is received to

do equity to the hardware hub. The roundabout shut end venture organization assessment material of the procedure hub is firm in light of the prescribed speculation from dissimilar hubs in VANETs. The circuitous trust assessment gives the hubs inside the system a chance to call a spade a spade the gathering of the new win vehicle hub.

They projected an "identity-based batch verification" strategy for vehicle to Infrastructure as well as "Vehicle to Vehicle" correspondence in VANET [16][17]. They embraced a one term administrator bolstered style, which disposes of the confirmation and broadcast expenses of endorsement for individuals key. It contracts the gross check interlude of a pot of substance marks, and its clump confirmation influence for marks from twofold vehicles are much rapider than of another PKI-based strategies. In constituent, the automobile allied data must be incognito from despiteful admittance, trust power can uncover the sender if contend shows up. The shortcoming of this plan is undefended on the replaying objection. An enemy may distort a diversion presuppose, for example, congested driving conditions, by gathering and putting away the vehicle messages and marks in the comparable confirmation. The side issue is doesn't give the hypotheses of non-revocation. A malignant vehicle can syllabus misinformed collection to honed new vehicles and untruth the liveliness when the trust power follows her/him by mark.

They drew consideration towards the security dangers present in the current IBV conspire and acquainted an enhanced plan with meet the security and protection necessities of vehicles [9]. The self-styled IBV ambition provides stability in the arbitrary prophet model. Over, the set look into of the would-be intention needs merely a tight permanent surrounded by of confederation and locating spreading calculations, autonomous of the quantity of messages. In spite of the favorable circumstances, the clump check may lose its suitability if aggressors send some invalid messages.

Regardless of the security accomplishment, the plan proposed by Tzeng does not address another essential issue of transmission collision. At the point when different hubs inside the same correspondence extend all the while attempt to show their messages, there happen the odds of transmission collision. To address the collision drawback, the present paper introduces the use of VeMAC protocol which works in a period opened structure. It is a TDMA construct convention which works with respect to the principle of one time slot allocation to active node.

3. FRAMEWORK MODEL AND PRELIMINARIES

3.1 Architecture components

The framework model of VANETs in a general sense contains TA, affixed RSUs at the road aspect, and portable OBUs prepared in vehicles as appeared in Fig 3 [1].

- In a communication network Trust Authority (TA) is totally trustworthy by all substances in the correspondence system. It gives enrollment and confirmation to stable RSUs and portable OBUs prepared on the vehicles. It parts the entire area into number of spaces, makes the group key and bunch signature materials for each territory, and in this manner sends it to the RSUs in the space.
- RSUs are deployed by TA at fixed positions along road or at any dedicated locations to accomplish and converse with vehicles in their correspondence range.

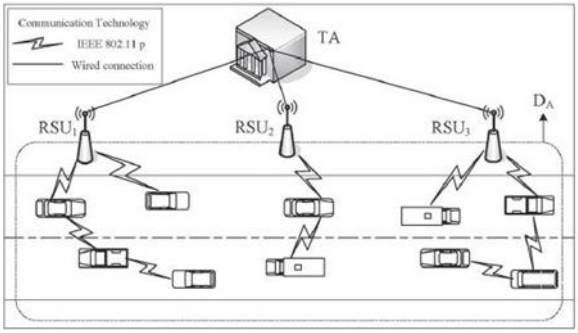

Fig 3: System Architecture

- OBUs are prepared on the running vehicles then that they telecast movement related standing data like area, rate, and bearing to support the street air and subsequently the entire security of driving conditions.

3.2 Security Requirements

Some of the principle difficulties of securing VANETs is communication security. This means to supply secure correspondence between vehicles, vehicles and Road Side Units i.e. (RSU). The security is a critical issue because the information transmission is propagated in open access environments.

A safe base for VANET ought to fulfill the accompanying prerequisites [3]: Any security framework should make sure that essential security benefits square measure gave in VANETs.

- **Authentication:** It is to guarantee if the messages are generated and delivered by authentic entities. To attain authentication, each vehicle needs to demonstrate its substantial personality to another vehicle.
- **Message Honesty:** Vehicles ought to have the capacity to distinguish if messages could debased or not amid the transmission. Something else, an assailant may supplant the security messages from automobile.
- **Non-disavowal:** No vehicle can shroud the way that a message is created and dispersed without anyone else. It is essential in the event of any mishap examination where the vindictive clients can't misdirect a RSU and can't escape if followed its message marks.
- **Identity privacy:** The genuine characters of vehicles ought not be uncovered to any ordinary message beneficiaries aside from TA to ensure the senders' secretive data.
- **Security Message Unlinkability:** None with the exception of TA can choose whether two diverse legitimate messages are delivered by the indistinguishable sender or not.
- **Wellbeing Message Unforgeability:** None can create an authentic wellbeing message without a RSU.
- **Tracebility:** In spite of the fact that the vehicle's genuine personality ought to be avoided RSUs and

different vehicles, yet TA ought to be able to recover or follow the vehicle's genuine character if there should be an occurrence of any liable of bringing about mischance or wrongdoing.

Table 1: Notation Used

Notations	Description
TA	Trust Authority
RSU	Road Side Unit
OBU	On Board Units
IBV	Identity based batch verification
Vi	The ith vehicle
ri	A random number
RID	Real Identity of Vehicle
T	Timestamp
M	Message sent by vehicle
||	Message concatenation operator
XOR	Exclusive OR
PPUB	Public Key of TA
AID	Anonymous identity
X	Private key
h	Hash function
P,Q	Generators of cyclic group G
H	Map to point hash function

4 PROBLEM AND PROPOSED WORK:

The paper involves the concept of batch verification where numerous messages signed may be confirmed at a single signature and confirmation cost. Firstly Zhang (2008) projected an "identity based batch verification" plan for V2I plus V2V correspondences in VANET [6]. They will embrace a erstwhile id based sign that takes out the confirmation as well as transmitting expenses of declaration for open key.

The problem arise with batch verification of messages is that there incurs a menace of transmission collision due to node mobility on channel. It is essential to keep away from collision on the channel to guarantee a quick and solid wellbeing messages trade. The pragmatic broadcast job gives an authority to act as witness for high-priority stability applications in VANETs. But in that there is less focus upon network performance so protocol is required to enhance the network performance in order to abate collision.

To elude collision issues, the VeMAC convention [10] is utilized, which likewise bolsters the multi hop broadcasting. Time is isolated to outlines comprising of a proceeding with assortment of mounted period time slots. VeMAC appoints disjoint arrangements of time slot to the vehicles to manage the transmission collisions resulted by node mobility on the channel. The time allocation is finished in such some way that every node should acquire specifically just once wring a frame on channel. On effort a time interval, a node keeps accessing it altogether consequent edges on channel unless a transmission collision is distinguished. There are largely 2 sorts of collisions discovered in transmission: Access Collision and therefore the merging collision. The access collision is observed when numerous hubs inside two hops of one another tries to accomplish the same accessible time space. While a merging collision happens when numerous hubs having the same time space get to be individuals from the same two-hop set (THS) because of hub portability.

The IBV plan comprises of three stages –

Stage1 "System initialization": TA instates and appoints every one of the parameters for every vehicle and RSU.

Stage2 "Anonymous identity generation module": The car inputs its inimitable real identity plus password into the tamper-proof device to permit the check of the verification module.

"The anonymous identity generation module" arbitrarily picks number ri then computes an anonymous identity AIDi which is composed of two parts AIDi,1 and AIDi,2 [9].

$AIDi,1 = ri\ P$

$AIDi,2 = RID \text{ XOR } H(ri\ Ppub)$

Stage3 Vi creates and inputs the message Mi to the tamper-proof device. With a present timestamp Ti, the message signature component computes the signature Si of Mi as shown below [9]:

$Si = (ri + xh(Mi \| AIDi,1 \| AIDi,2 \| Ti))Q$

The final output message given by tamper proof device is {AIDi , Mi, Si, Ti}and it is sent by Vi to adjacent RSU and vehicles.

Assume N be the number of primarily available time slots in a frame, K shows the number of challenging nodes.

Xn as the aggregate numeral of nodes which achieve a time slot inside n frames. The below shown transition probabilities sustenance Xn as a static discrete-time Markov chain:

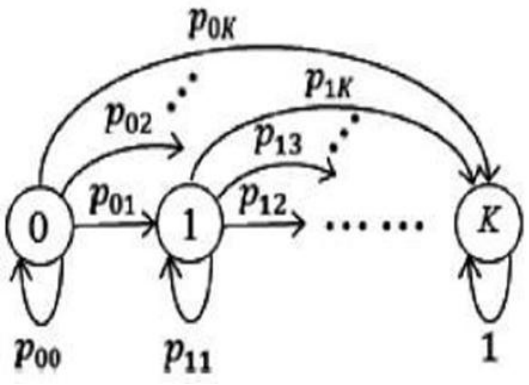

Fig 4: "Markov chain for Xn when K≤N" [10]

If K ≤ N

$$p_{ij} = \begin{cases} \frac{W(j-i,K-i,N-i)}{(N-i)^{K-i}}, & 0 \le i \le K\text{-}1,\ i \le j \le K \\ 1, & i = j = K \\ 0, & \text{others} \end{cases} \quad (1)$$

Wherever W (l,u,v) be the quantity of methods thru which l nodes may attain a time slot specify that u contending nodes are present which haphazardly select a time slot amongst v accessible time slot as shown in Eq. (1) and Eq. (2) [10].

"Markov chain" is defined as aleatory strategy with "Markov property". The expression "Markov chain" intimates the get-together of sporadic variables like a procedure experiences, by the Markov property depicting sequential reliance just amid circumscribing phases. It may along these lines can be utilized for delineating frameworks that take after a chain of related occasions, where whatever ensues following depends just on the present condition of the structure [25]. Conventionally the term is held for a methodology with a distinct game-plan of times, i.e. a "discrete-time Markov chain (DTMC)" as showed up in fig 4 and 5. It is broadly connected in numerous fields, for example, market prediction [21,22], traffic transition prediction [23], traffic situation prediction [24], transmission of packet delay prediction [2]. So in this paper it is utilized for allotting the time slot to the vehicles with a specific end goal to lessen the transmission collision.

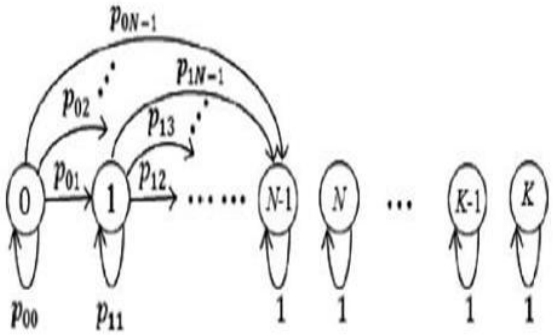

Fig 5: "Markov chain for Xn when K>N" [10]

If K > N

$$p_{ij} = \begin{cases} \frac{W(j-i,K-i,N-i)}{(N-i)^{K-i}}, & 0 \le i \le N\text{-}1,\ i \le j \le N\text{-}1 \\ 1, & i = j,\ N \le i \le K \\ 0, & \text{others} \end{cases} \quad (2)$$

Consider P and Pn as the one-step and n-step transition probability matrix respectively.

It is given that at first all nodes are battling for time slots, for example, X0= 0 with possibility 1, the unrestrained possibility dissemination of Xn is spoken to by the principal column of Pn as shown in Eq. (3) [10].

That is,

$$p(X_n = i) = P^n_{1,i+1}, i = 0, \dots\dots\dots, K \quad (3)$$

Eq. (4) [10] shows the possibility with which that all nodes obtain a time slot inside n frames.

$$F_n^{all} = p(X_n = K) = P^n_{1,K+1} \quad (4)$$

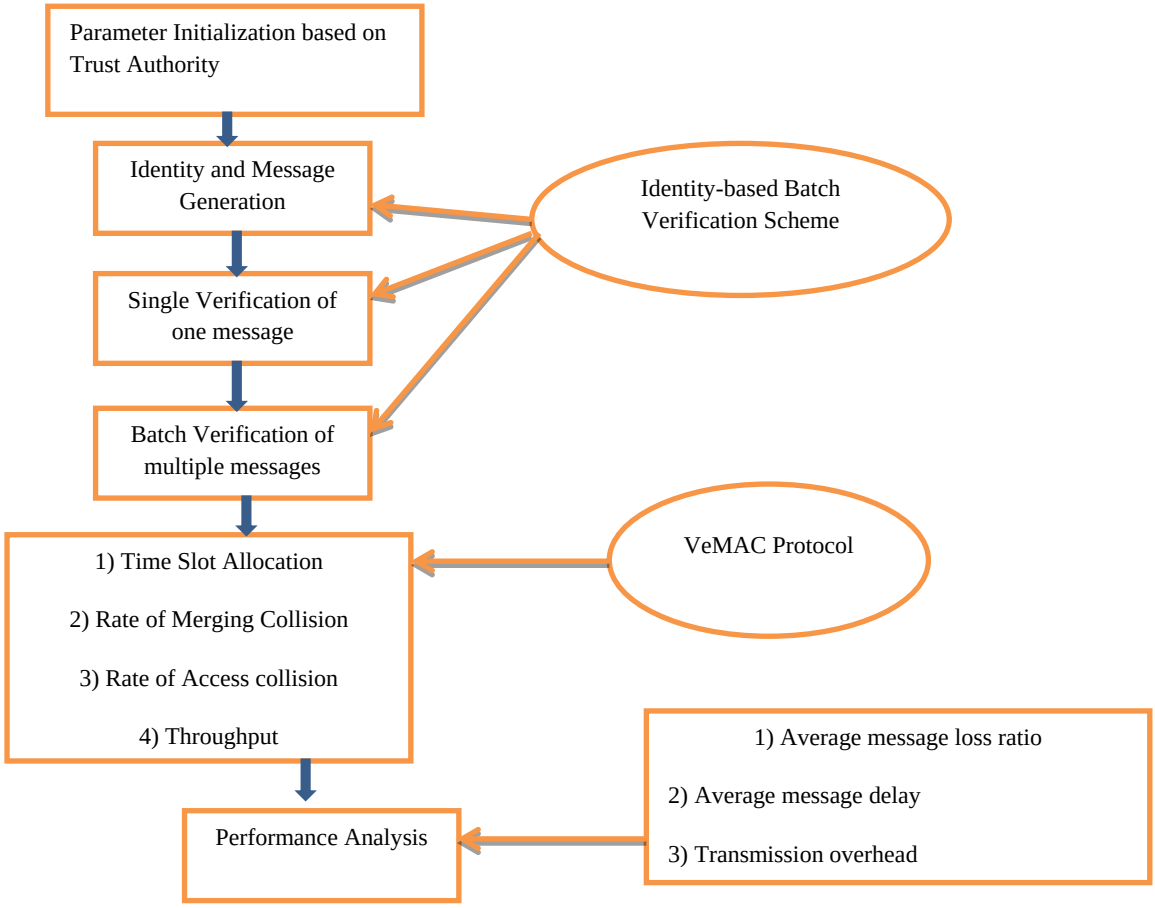

Fig 6: Flowchart of Projected work

The average numeral of nodes that attain a time slot inside n frames as shown in Eq. (5) [10]:

$$\text{[illegible]}_n = \sum_{i=0}^{K} i\, P_{1,i+1}^{n} \quad (5)$$

The proposed approach works as follows in Fig 6:

- The approach starts with the parameter initialization based on TA.
- Then identity and message are generated

Then the VeMAC protocol deals the following factors:

- timeslot allocation is done
- Rate of merging collision
- Rate of access collision
- Throughput
  - Finally the performance analysis is done using following parameters
  - Transmission overhead: The transmission overhead to be the numeral of bits, conversed for a message, that does not connote the data bits of the message
  - "Average message loss ratio": It is the proportion of quantity of message disposed of to the quantity of messages got.
  - Average message delay: The deferral of a system determines to what extent it takes for a bit of information to traverse the system starting with one endpoint then onto the next.
  - Single confirmation of one message and then the batch confirmation of multiple messages is performed using IBVS.

5 SIMULATION RESULTS

The proposed IBV with VeMAC scheme has been simulated in MATLAB and the execution of the proposed plan has been analyzed with veneration to three different parameters- "Average Message Delay", "Average Message Loss" and "Transmission Overhead". The performance of the proposed scheme has been compared in contrast to the prevailing scheme is given below in three different graphs.

As it can be seen in Fig 7 shows the rapport between "Transmission Overhead" with "the numeral of messages received by a receiver in 30 seconds" is given. The graph displayed in green displays the " transmission overhead" against the "number of messages received by a RSU in 30 seconds" in the existing IBV Scheme and the pink graph displays the improvement with the introduction of VeMAC Protocol in the prevailing IBV Scheme. It is very clear from the graph given in Fig 7 that with the introduction of VeMAC Protocol with the prevailing IBV Scheme the transmission overhead has improved to a prodigious range. For example with IBV Scheme for receiving approximately 4x104 messages in 30 seconds more than 6 Mbytes of transmission overhead is required but with the introduction of VeMAC Protocol with prevailing IBV Scheme the equivalent outcome can be accomplished with less than 4 Mbytes of transmission overhead.

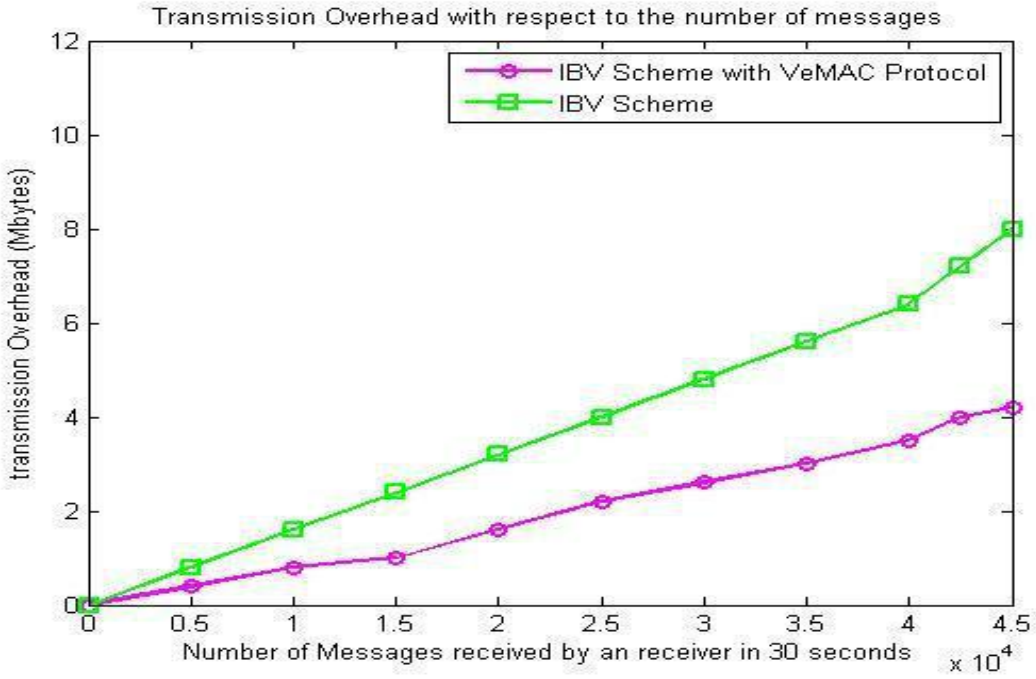

Fig 7: "Transmission Overhead with respect to the number of messages

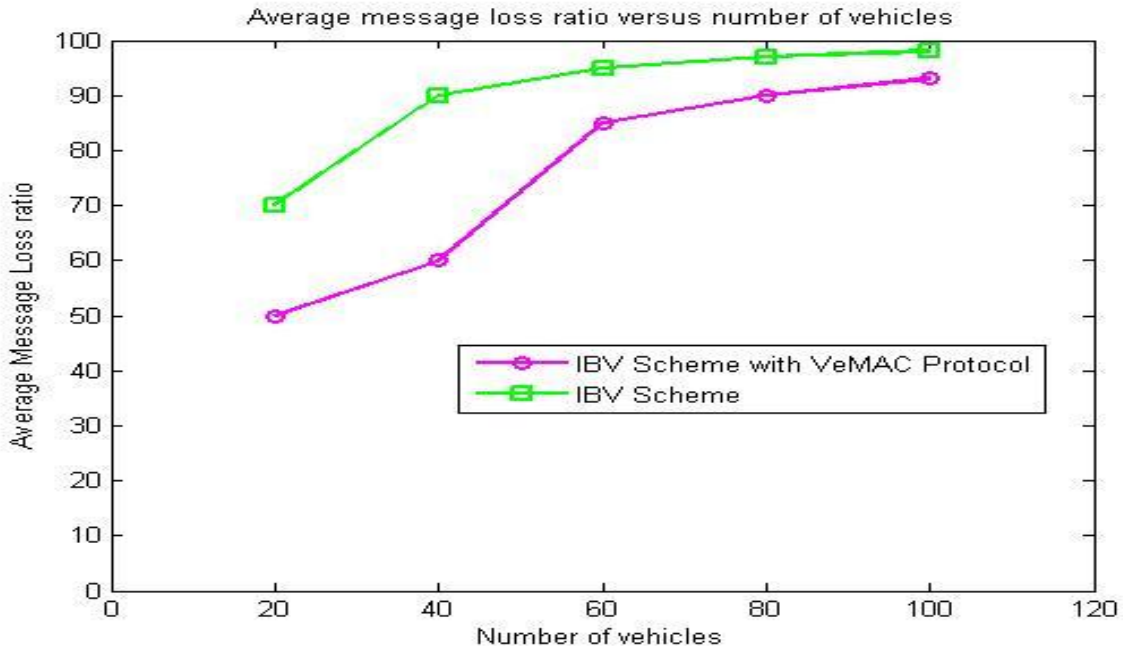

Fig 8: "Average message loss ratio versus number of vehicles

As the Fig 8 shows the rapport between "Average Message Loss Ratio" against "Number of Vehicles" is analysed. Once again the graph epitomized in the green envisages the statics with IBV Scheme whereas the graph in the pink envisages the statics of IBV Scheme with introduction of VeMAC Protocol. From the graph one can effortlessly make out that the "average message loss ratio" with veneration to the "number of vehicles" has abridged to a prodigious range with the introduction of the VeMAC Protocol in the prevailing IBV Scheme. For example average message loss ratio was approximately 70 for 20 vehicles with IBV Scheme and the same was abridged to 50 in contrast to 20 vehicles.

As it can be seen in Fig 9 shows the rapport between "Average Message Delay" against "Number of Vehicles" is analyzed. Once again the graph epitomized in the green envisages the statics with IBV Scheme whereas the graph in the pink envisages the statics of IBV Scheme with introduction of VeMAC Protocol. From the graph one can once again effortlessly conclude that the amount of "average message delay" has abridged to a prodigious range with the introduction of the VeMAC Protocol in the prevailing IBV Scheme. For example average message delay was approximately 10 in contrast to 100 vehicles with IBV Scheme and the same was abridged to approximately 1/10th

with the introduction of VeMAC Scheme in the prevailing IBV Scheme.

The outcomes illustrate that the IBV scheme with VeMAC provides improved performance since the "transmission overhead", the "average message loss ratio" and the "average message delay" are abridged in contrast to other prevailing scheme.

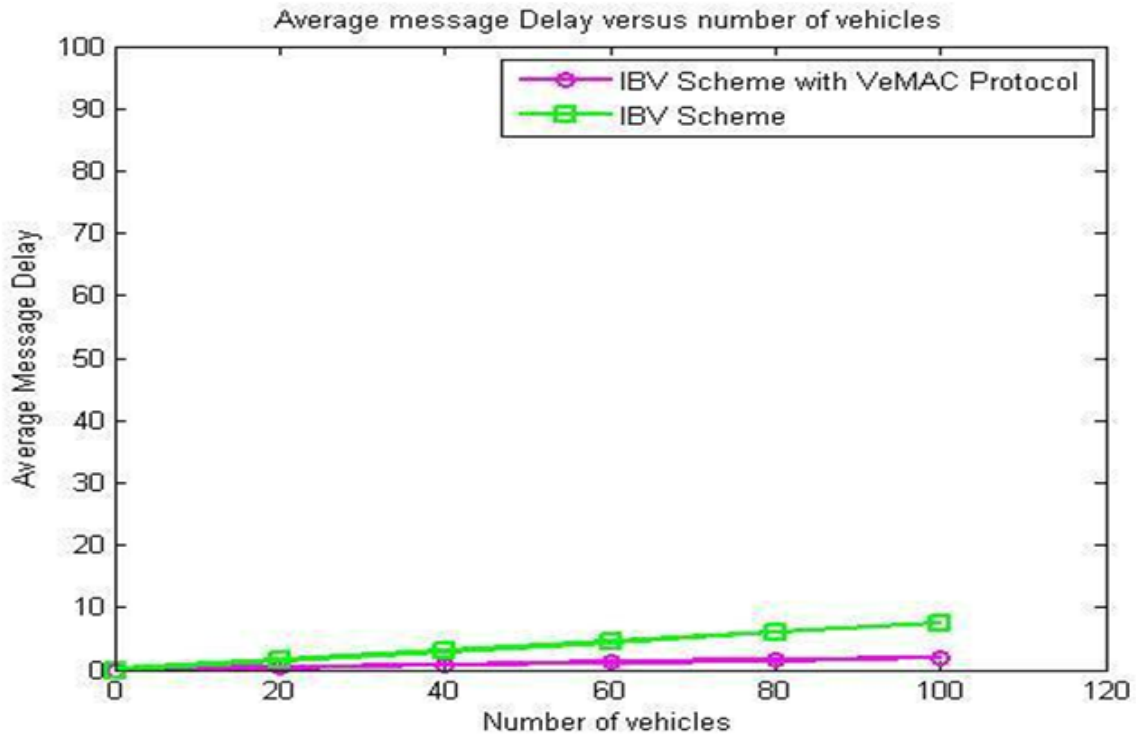

Fig 9: "Average message delay versus number of vehicles

6 CONCLUSIONS AND FUTURE WORK

Vehicular Ad Hoc Network is a auspicious innovation, which gives assailants the chances to challenge the system with their malignant assaults. New mechanisms have been developed to deal with the inherent features of these networks. This paper identifies the security requirements and addresses the transmission collisions incurred due to node mobility in the network. . The VeMAC is able to provide proficient one-hop and multihop broadcast administrations on the channel by utilizing certain affirmations and taking out the shrouded fatal issue. In IBV when a collector needs to affirm countless messages, the batch based confirmation for different message marks is more effective than one after another single check. However there is less focus on network performance. So in this paper, IBV scheme with VeMAC has been used to combine the advantages of both IBV and VeMAC scheme, with the aim to reduce transmission collision which ultimately improves the network performance. The proposed work is simulated and the results obtained indicate the reduction in transmission overhead, message delays and message loss ratio. More work can be done to enhance the performance of network by using different MAC protocols and comparison can be made with the proposed hybrid algorithm.

7 ACKNOWLEDGMENTS

The paper has been composed with the kind assistance, guidance and support of my department who have helped me in this work. I would like to thank all the people whose encouragement and support has made the fulfillment of this work conceivable.

8 REFERENCES

[1] Zhu, X., Jiang, S., Wang, L., and Li, H. (2014) "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks," IEEE Transactions On Vehicular Technology, Vol. 63, No.2, pp. 907 – 919.

[2] Hafeez, K.A., Zhao, L., Ma, B. and Mark, J.W. (2013) „Performance Analysis and Enhancement of the DSRC for VANET‟s Safety Applications," IEEE Transactions on Vehicular Technology, Vol. 62, No. 7, pp. 3069-3083.

[3] Varshney, N., Roy, T. and Chaudhary, N. (2014) "Security Protocol for VANET by Using Digital Certification to Provide Security with Low Bandwidth," International Conference on Communication and Signal Processing, IEEE, pp. 768-772.

[4] Chim, T.W., Yiu, S.M., Hui, L.C.K. and Li, V.O.K. (2011) "SPECS: Secure and privacy enhancing communications schemes for VANETs," Attribution 3.0 Hong Kong License, Vol. 9, No. 2, pp.189-203.

[5] Zhu , H., Lin, X., Lu, R. and Ho, P.H. and Shen, X(Sherman). (2008) "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks," IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings, pp.1436-1440.

[6] Zhang, C., Lin, X., Lu, R., Ho, P.H. and Shen, X(Sherman). (2008) "An Efficient Message Authentication Scheme for Vehicular Communications," IEEE Transactions on Vehicular Technology, Vol. 57, No. 6, pp. 3357-3368.

[7] Lee, C.C. and Lai, Y. M. (2013) "Toward a secure batch verification with group testing for VANET," Wireless Networks, Vol. 19, No. 6, pp.1441-1449.

[8] Zhou, A., Li, J., Sun, Q., Fan, C., Lei, T. and Yang, F. (2015) "A security authentication method based on trust evaluation in VANETs," EURASIP Journal on Wireless Communications and Networking, Vol. 1, pp. 1-8.

[9] Tzeng, S.F., Horng, S.J. , Li, T., Wang, X., Huang, P. H. and Khan, M. K. (2015) "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET," IEEE Transaction on Vehicular Technology, Vol. 99.

[10] Omar, H.A., Zhuang, W. and Li, L. (2013) "VeMAC: A TDMA-Based MAC Protocol for Reliable Broadcast in VANETs," IEEE Transactions On Mobile Computing, Vol. 12, No. 9, pp. 1724-1736.

[11] Hadded, M., Zagrouba. R., Laouiti, A., Muhlethaler, P. and Saïdane, L. A. (2014) "An Adaptive TDMA Slot Assignment Strategy in Vehicular Ad Hoc Networks," Journal of Machine to Machine Communications, Vol. 1, No. 2, pp. 175–194.

[12] Omar, H.A., Zhuang, W. and Li, L. (2011) "VeMAC: A Novel Multichannel MAC Protocol for Vehicular Ad Hoc Networks," Computer Communications Workshops (INFOCOM WKSHPS), IEEE, pp. 413 – 418.

[13] Rehman, S., Khan, M. A., Zia, T. A. and Zheng, L. (2013) "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges," Journal of Wireless Networking and Communications, Vol. 3, No. 3, pp. 29-38. [14] Liu, B. and Zhang, L. (2013) "An Improved Identity-based Batch Verification Scheme for VANETs,"5th International Conferenceon Intelligent Networking and Collaborative Systems, IEEE pp. 809-814.

[15] Huang, J.L., Yeh, L.Y. and Chien, H.Y. (2011) "ABAKA: AnAnonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," IEEE Transactions On Vehicular Technology, Vol. 60, No. 1, pp. 248-262.

[16] Zhang, C., Lu, R., Lin, X., Ho, P. H. and Shen, X. (2008) "An efficient identity- based batch verification scheme for vehicular sensor networks," in Proceedings of the 27th IEEE International Conference on Computer Communications (INFOCOM'08), pp. 816-824.

[17] Zang, C., Ho, P. H. and Tapolcai, J. (2011) "On batch verification with group testing for vehicular communication," Wireless Networks, Vol. 17, No. 8, pp. 1851-1865.

[18] Networking Lab Kyung Hee University, "VANET Architecture,"http://networking.khu.ac.kr/layouts/net/research/res33.htm (Accessed: March 2016).

[19] Raghul, G., Dhayabarani, R., Vivek, R. (2014) "ppt on Dedicated Short Range Communication," http://www.slideshare.net/asdfadmin/24-42893721 (Accessed: March 2016).

[20] Guo, J. and Balon N. (2006) "Vehicular AdHocNetworks and Dedicated Short-Range Communication," University of Michigan – Dearborn.

[21] Chief Editor: Cheng, H.X. (1993) Market Occupancy (Markov) Forecasting Methods, 80 Practical Market Forecasting Methods", Peking Economic Institute Press.

[22] Zhaopeng, M., Li, L. and Peng, L. "Study on Computer Sales Market Model Based on Markov Analysts," Decision and Decision Support Synem, Vol. 1, pp. 88-93.

[23] Zude, C. (1994) "A study on Shifting Traffic Volume of the Vehicular Ferry and Yangpu Bridge by Grey Theory and Operations Research Method," Journal of Maritime University, Vol. 03.

[24] Tang, H., Wu, H. and Meng, J. (2012) "The Model Analysis of VANET at Intersections Based on Markov Process," State Key Laboratory of Rail Traffic Control And Safety, Beijing Jiaotong University, Beijing, China.

[25] Fan, C.I. , Sun, W.Z., Huang, S.W., Juang, W.S. and Huang, J.J. (2014) "Strongly Privacy-Preserving Communication Protocol for VANETs," Ninth Asia Joint Conference on Information Security IEEE, 119 – 126. Parno, B., Perrig, A. and Gligor, V. (2005) „Distributed detection of node replication attacks in sensor networks", Proceedings of 2005 IEEE Symposium on Security and Privacy (S&P'05), pp.49–63.