A SURVEY PAPER ON CONGESTION CONTROL TECHNIQUES IN VANETs

Mantasha Haseeb
Dept. of Electronics &
Communication Engineering
SHUATS, Allahabad, India

A.Ashok
Dept. of Electronics &
Communication Engineering
SHUATS, Allahabad, India

Neelesh Agrawal
Dept. of Electronics &
Communication Engineering
SHUATS, Allahabad, India

Abstract- A network of vehicles in adhoc nature i.e. Vehicular Ad-Hoc Networks (VANETs) are expertise and uses moving cars or some other vehicle eg: bus in a network as nodes to craft a system of mobile. Networks of Vehicles in adhoc nature turn every car or vehicle participating with a wireless router, allowing cars or buses to connect and craft a network with a spacious range. Networks of Vehicle in adhoc nature are developed for ornamental driving security and comfort of automotive users. When traffic occurs, it is obligatory to diminish the load of the beacon to keep definite quantity of the vacant bandwidth for the messages which are ED messages as they cart information which is time-critical of high importance. Therefore, the congestion control remains one of the most exigent problems of these networks. This paper surveys some techniques on congestion control, which are divided into three categories: Rate adaptation, Media access control which is (MAC) and trajectory based Forwarding schemes for VANETs.

Keywords-ADHOC Networks, VANETs, Congestion Control, Rate Adaption, MAC, Trajectory Based Forwarding.

I. INTRODUCTION

Wireless means signal broadcast via radio waves as the intermediate as an alternative of wires [1]. With the help of wires, cables or any other form of electrical conductor's wireless communication engage the transmission of information in excess of a distance [2]. With VANETs (Vehicle Ad-Hoc Networks) are poised of vehicles such as car or bus equipped with sophisticated wireless communication devices lacking of any base stations. Every vehicle equipped with VANETs gadget will be a node in the ad-hoc network and can receive and impart others messages through the wireless set of connections [3]. The key topic for research community and industry is networks of vehicules (VANETs). Networking of Vehicle enables the sustain of traffic safety applications designed to decrease the amount of accidents on the roads [4].

To barter traffic information among vehicles in a scalable fashion is an important setback that has to be solved in Network of Vehicles [5]. The structure consists of connections between smart vehicles equipped with sensors [6]. For the expansion of networks of vehicles known as (VANETs) a large number of appealing and considered necessary applications of Intelligent Transportation Systems (ITS) are stimulated [7]. Future automotive companies and governments in numerous countries are now contemplating a large-scale deployment of intelligent system of the transport [8].

We judge different kinds of messages in vehicular networks: Data Messages, Beacon Messages and the Event Driven security Messages. Those which are taken into concern in the bulk of traffic control algorithms are the preceding two. In fact, when a vehicle or the road infrastructure discovers a critical situation Event-Driven Safety Messages (ED) called also Critical Event Messages, or Warning Messages, are sent. These messages must be relayed with no delay, for the reason that they carry time crucial information of high importance, while Beacon Messages called also Periodic Messages, are broadcasted periodically (every 2 seconds) by all nodes to forward and receive information about the network [6]. Figure 1 shows the Traffic Control Parameters i.e. also known as congestion and how traffic can be controlled or reduced by some of the parameters of congestion.

Figure 1: Traffic Control Parameters

II.CONGESTION CONTROL TECHNIQUES:

The traffic control techniques can be considered into three foremost groups namely: Rate adaptation, Media access control and trajectory based forwarding schemes, but in this critical survey paper we will focus the three techniques in detailed [6].These techniques are further discussed below:

III. SURVEY STUDY

A. RATE ADAPTATION:

In the category of rate adaption, in order to generate a new flow rate away from congestion zone we find algorithms that regulate the flow rate in accordance to the condition of the network.

(1) Congestion Control in Vehicular Ad Hoc Networks [9]:

UBPFCC (Utility-Based Packet Forwarding and Congestion Control) basic idea, instead of minimally assigning the alike rate to all nodes, and more efficient to allocate data rates based on (average) utility of data packets send out via vehicle. To consume a generously proportioned share of the vacant bandwidth nodes transmitting information having high utility for the VANET is allowed. The (UBPFCC) based on these parts:

- Rate of the data based explicitly with utility of transmitted or remit data packets is alleged by all nodes.
- The information packet with the utmost utility is dequeued from the packet queue whenever a fresh data packet desires to be preferred for transmission.
- Row packet with partial limit length of K packets of data. If the row extent exceeds K upon enqueueing a fresh packet of data, the packet data with the tiniest utility is dropped.
- Broadcast packets data are received that can't be delivered to an application on node and are accumulated in a detach queue and re-transmitted as long as capacity is vacant and the packet's time-to-live value is not expired.

Result and Discussion: A stochastic model of a distinctive scenario of highway is the UBPFCC, was executed in the ns-2 simulator. The presentation of a VANET via UBPFCC is evaluated with alike reference system (REF) lacking UBPFCC by network simulations. A microscopic simulation of traffic has been put into operation in the ns-2 simulator, via a Cellular Automaton (CA) approach to bring into play a realistic mobility model. Arrival period are supposed to be Poisson distributed, preliminary time gaps among adjacent vehicles are consequently selected from an exponential distribution.

(2)DRCV (Distributed Rate Control Algorithm for VANETs) [10]:

The well known fact is that TCP is not apt for traffic control in VANETs. Even despite the fact that a numeral of alternative of TCP have proposed, they didn't assemble the desires of security message dissemination. There are limited studies spotlighting on congestion control for security messages one of them is (DRCV) a distributed light-weight traffic control algorithm customized for security messages. DRCV first monitors and calculate approximately channel load and reins the rate of outgoing cyclic packets. [4] The DRCV algorithm consists of the following main parts:

- **Monitoring the channel:** Channel monitoring is presented periodically in a scattered way, i.e. all nodes nearby monitors channel load constantly.
- **Estimation of the future load:** At the finish of all monitor intervals, estimation of the load in the next monitor interval is made.
- **Action to be taken:** Action is taken by all nodes.

Considering two types of metrics for channel load:

- Data Packet Rate: 1) All nodes dynamically locate the collective end channel load of cyclic messages produced by itself and its neighbors. In the first stage DRCV in fact partitions the channel capacity among ED and cyclic messages. 2) All nodes close by controls its sending rate of cyclic messages in order to arrive at comprehensive target channel load set in the first stage.
- CBT

Results and Discussion: Simulations conceded out with usefulness of DRCV demonstrated in dropping the channel load and getting better packet reception probabilities. The scenario of simulation grades having two short bursts of ED messages, is to emphasize the benefits of DRCV, i.e. in all burst ED messages sent at the speed of 10Hz for 500ms and observed that when a burst starts, DRCV-FD right away cuts the congestion load by half, and when no ED message is detected, DRCV-FD linearly boost the load of cyclic messages equipped the predefined utmost threshold. Results observed that DRCV increases the reception possibility with reference to 15% contrast to the crate without rate control.

Table 1: Packet Reception Probabilities

Simulation tool ns-2.31	1st ED burst	2nd ED burst
No Rate Control	74.98%	75.34%
DRCV-P	88.92%	91.31%
DRCV-FD	88.56%	90.46%

(3) Congestion Control Framework for Disseminating Safety Messages in VANETs [11]:
The congestion control outline can be separated into three main parts:

(a) Congestion Detection and Congestion Control (CC): The principle of congestion revealing is to monitor communication network channels and become aware of congestions. Two sort of traffic revealing methods in CC approach are ED detection and MB detection.
Event Driven Detection: This scheme monitors the safety messages and come to a decision to commence the congestion control whenever a high priority security message is detected. Detection of event messages can be expressed in Figure 2 with code.

- Queue freezing is done in Congestion Control
- A security message is locally generated
- A security message is received from another station
- Freeze every bit of MAC queues excluding for the security queue

```
/* Congestion Control with Queue freezing */
If ((A safety message is locally generated ) or (A safety message is received from another station ))
{
Freeze all MAC queues except for the safety queue;
}
```

Figure 2: Pseudo Code of Event Driven Detection

M Based Detection: Scrutinizing of CCH communication based lying on packets outlet queues. The outlet is jam-packed if messages in the log jam go beyond a defined threshold. Nodes can have up to eight log jams of which all represents a different Access class, which is often referred to as Traffic class.

(b) Arrangement algorithm: Adaptation of Earliest Deadline First (EDF) which is priority-based to plan uni-priority of ED security messages. Each packet gives main concern and time limit (maximum latency) in VANETs. The scheduler basically transmits packets in increasing order remaining deadlines and priority-based EDF arrangement algorithms supply the packets according to their main concern and deadline. The priority-based EDF is a forceful arrangement algorithm worn in real-time relevance systems. Priority of EDF arrangement algorithm is clear in Equation (1) and (2) are:

$$\text{Packet Queue} = \text{Priority} + \text{Deadline} \quad (1)$$
$$\text{Deadline} = \text{Packet Arrival} + \text{Max Latency} \quad (2)$$

The node has three ED security messages with high precedence message need to be transmit e.g. line of traffic change caution, forward collision and pre-crash sensing. The three of ED security messages arrival at different time. The line of traffic change caution arrived at time 1, forward collision arrived at time 2 and precrash sensing arrived at time 3. Based on EDF arrangement algorithm defined in Equation (1) and (2), the packets queue is C A B (where the lower packet queue is a high precedence to transmit).

(c) Rebroadcasting systems: To disseminate ED security messages, such as to inform drivers in case of hazardous events are the most significant criteria of security application. Blindly broadcasting packets may go ahead to numerous contention and crash in broadcast among neighboring nodes for the reason that of the joint wireless medium. This predicament is from time to time referred to as the transmit storm or blind flooding. This flooding method causes a lot of severance. A latest broadcast aim in traffic control to ensure high consistency of ED security messages. This televise system also performs low over head by means of dropping retelevise redundancy in a high-density network.

Result and Discussion: A scalable congestion control spotlight on disseminating event-driven security messages in VANETs. CCH in intense network easily congested by periodic updates of periodic security messages and televise storm from critical event security messages. The loom of congestion control is the best solutions to solve congestion wireless communication channel in VANETs. Traffic construction will scan the messages queues and scrutinize outlet communications based on defined threshold. It also becomes accustomed priority-based EDF arrangement algorithm in traffic control. To offer reliability presentation for ED security messages, a new rebroadcasting system is developed. Traffic control made-up to reduce the outlet load in order to meet the QoS requirements of the wireless set-up recital.

(4) Performance Evaluation of Beacon Congestion Control Algorithms for VANETs [8]:

Three beacon traffic control algorithms:

- Rate control,
- Power control, and
- Joint power + rate control.

The following three aspects incorporate these algos

- First, they scrutinize the outlet conditions during the monitoring interval T.
- Secondly, they originate the estimated outlet load from the observed outlet conditions.
- Third, they fine-tune the transmit power and/or the beacon rate to be used in the next monitoring time.

Result and Discussion: The feat of the beacon traffic control algorithms by performing simulations of ns-2 for an assortment of intersection scenarios and at unlike levels of vehicle compactness. No traffic rule pertains, ratio of the CBT rises drastically with the intersection size. The algorithms obtain a higher reception rate for ED caution messages than when no traffic control is exercised. Traffic control algorithms recovers the reception charge for the caution messages and able to mitigate traffic on the wireless medium.

(5) Congestion Control Algorithm in VANETs [3]:

This algorithm of traffic control ensures high reliability and timely deliverance of distributed ED security messages. The algorithm of traffic control can be detached into two core parts: ED detection and MB detection.

Event-Driven Detection: Method examined the event-driven security message and whenever event-driven security message is spotted or generated it settled on to start the congestion i.e. traffic control algorithm. The congestion i.e. traffic control will start on instantaneously the queue freezing mode for all MAC transmission queues apart from the event-driven security message. The priority of minor messages such as beacon messages release should be freeze in command to send event-driven security message with minimum delay.

MB Detection: The detection will supervise CCH outlet based on packets outlet queue. The CCH outlet is in traffic when number of messages in the row goes beyond a defined threshold. Row with a length of five beacon messages is satisfactory to used for 802.11p beaconing. Traffic control algorithm, will discard a beacon security messages at any time the length of packet row more than five beacon security messages.

Result and Discussion: Studied the traffic problem in support of event-driven security messages in VANETs background. The congestion i.e. traffic control algorithm proved as well-organized mode for disseminating event-driven security messages in impenetrable network scenario. With widespread and reasonable simulation results traffic control algorithm achieved the most excellent in terms of packets delay ratio. The event-driven security messages must distribute to all neighbouring node without any stoppage. A single overdue of event-driven security messages might result in failure of life.

(6) VANETs to Be Beacon or not to Beacon? [12]:

The basic idea of the BEACONED (periodic) algorithm is that

(a) Each node estimates the position of its neighbours.
(b) Estimated spot is then used to decide whether a message should be forwarded or not.
(c) An aim at trading-off the number of transmitted messages is the forwarding decision and the probability to inform the vehicles.

PERIODICLESS algorithm is that:

Based on two ideas:

i) To support the forwarding conclusion.
ii) Set up waiting time before the message forwarding.

The underlying principle behind the proposal of letting the choice depend on the distance is the consequent: when a node pay attention to the message for the first time and its distance from the send out node is small, then the supplementary exposure that can be pull off by re-broadcasting the message is also little thus, the conclusion to forward the message ought be taken with low probability. The character of the waiting time is to permit nodes to take note for new scopies of the broadcast message: this yield to a superior estimate of the less significant relay distance, which is then worn to tune the forwarding decision progression.

Result and Discussion: As the outlet utilization due to the beaconing is very low, the use of a jittered beacon broadcast keeps collisions of beacon messages negligible. As an outcome, when the wireless outlet is error-free, in every periodic interval, nodes gather complete information of their neighborhood. The design space of televise communication services for Network of Vehicles, considering two kinds of algorithms: the PERIODICLESS one, which relies solely on instantaneous information on vehicles position, and the PERIODIC one, that maintains and exploits longer-term knowledge of the vehicular network topology. In the case of ideal wireless outlet, by properly tuning the system parameters both algorithms accurately propagate a televise message. Moreover, if the beaconing overhead is neglected, the PERIODIC approach is more efficient in terms of the outlet utilization.

B.MEDIA ACCESS CONTROL (MAC):

The media access control category algorithms work differently. These algorithms use different techniques of media access according to the state of the network. There are several algorithms which are discussed below:

(1) VC-MAC: A Cooperative MAC Protocol in Vehicular Networks [13]:

The etiquette is on the IEEE 802.11 coordination function which is distributed, but (RTS/CTS) exchange is omitted because it is not necessary in televise mode. The whole procedure is composed of four components:

a) *Period of Gateway's televised:* in the gateways televise period, the gateway televise the packets received from its own upper layer to the vehicles in its range.

RI

Frame Control	User ID	Time Sent	CRC

DI

Frame Control	List of Neighbors	CRC

Figure 3: Format of RI and DI

b) *Period of Information switch:* Back off to dispatch out messages of prospective relays and potential ends randomly to update their neighbors of their life and use their messages to accumulate the outlet state and topology information indispensable in the following part of the protocol done in the information exchange period.

RRTS

Frame Control	Duration	Multiple Destination Address	CRC

RCTS

Frame Control	Duration	Destination Address	CRC

Figure 4: Format of RRTS and RCTS

a) *Assortment phase of Relay locate:* The relay assortment is beneath the guidance of the theoretical scrutiny and with the expectation of maximizing spatial reusability and user diversity. Then, in the relay set assortment phase, an estimated optimal relay set is selected from all prospective relay nodes in a distributed manner by leveraging the backoff mechanism.

b) *Phase of Data forwarding:* The packets received from the right of entry to possible ends within its transmission series. Finally, in the data-forwarding phase, the certain relays forward (or televise more actually).

Results and Discussion: 1) Extention of the Relay and AP (Access phases) of the end. The extention of the relay and access phases of the end affects the procedure performance by affecting the accident probability of RI and DI messages.

2) Extention of the phase of the Relay-Selection is important cause affecting the result of relay selection. For diminutive phase of the relay assortment, achievable relays that should have been selected in the relay locate may not have enough time to finish their backoff procedure; thus, they cannot be selected to forward data. The simulation completed by ns-2 and experiments are accomplished with version2.29.

(2) A Probability Based MAC Channel Congestion Control Mechanism for VANET [14]:

In traditional 802.11 DCF (Distributed Coordination Function), the value of *CW* has the minimal value (*CWmin*). After each packet impact, the *CW* will be twice over until achievement of the maximum *CWmax*. After all victorious transmission, the *CW* will be retune to *CWmin* in spite of the network conditions such as the number of recent rival vehicles, this mode tends to work fit when there are merely a few competing vehicles. When the number of rival vehicles increases, it will be shown to be ineffective considering as the new packet collisions can potentially arise and cause major performance deterioration. Subsequently even the vehicles has increased to a large value, the vehicles will use the same initial *CW*.

Result and Discussion: A lot of packet collisions occur as a result, and the packet loss probability is increased. Since vehicle uses *CW* to control the back-off window, the optimal setting of *CWmin* will affect the performance. In 802.11 DCF, the *CWmin* size is fixed (32 slots in DSSS 802.11b) regardless of the number of contending vehicles. Each number *N* of vehicles, there is an optimal value of *CWmin*. To adapt the *CWmin* according to the number of vehicles and data traffic, a simple novel scheme (called PCC, Probability based Congestion Control) to decrease the channel congestion problem. The PCC mechanism advantage over broadcasting is that there is a momentous cutback in channel congestion and packet collisions. The central idea of PCC system is that, in charge to diminish the number of collisions, the new *CWmin* size for each vehicle is carefully selected according to the number of contending vehicles and probabilistic model; this new *CWmin* value will maximize the channel utilization and the throughput. The new *CWmin* value should be increased linearly with the number of cars i.e. vehicles N. The PCC mechanism achieves relatively good performance compared to mechanisms based on fixed contention window (*CWmin*) size.

(3)Multi priority supported MAC [7]:

MAC format primarily rely on the IEEE Standard 802.11e to allocate different precedence's of application packets to admittance the DSRC channel. However, the throughput of system saturation and most favourable utilization of the WAVE outlet are not argued in the standard provision of WAVE. Due to set length of the CCH period, it is incapable to certify the reliable and real-time transmission of the security packets in an opaque node environment. In case of this type, the unremitting packet collision and backoff on the outlets will drastically reduce the effectual throughput of CCH. A multi-priority supported p-persistent (MP) MAC procedure to guarantee the prioritized transmission of the security packets, and challenge to maximize the saturated throughput on CCH by optimizing the transmission probabilities of dissimilar priority packets. Based on best possible channel access probabilities, a variable interval of CCH and SCH system is proposed to improve the channel utilization. Moreover, an ACK system is devised to confirm the reliable transmission of the security packets and avoid the collisions of simultaneous ACK packets. A slotted time based on p-persistent MAC system and an outlet reservation mechanism is there to avoid outlet collision on CCH and SCHs. The construction of the proposed MP MAC system in which the worldwide synchronized outlet coordination system based on the UTC is innate from IEEE 1609.4 to synchronize the time frame along with all vehicles, with the assist of RSUs and the Global Positioning System (GPS). The interval time synchronous is more divided into the variable intervals of CCH and SCH according to traffic atmosphere. The interval of CCH consists of the random access time and the ACK time. At the conception of the random access time, the RSU showed a MP packet piggybacked with the finest amount of CCH time, ACK time and the instruct of nodes turning over ACK packets to the vehicle nodes beneath its radio exposure. Receiving nodes will fine-tune the CCH time and the ACK time accordingly. During random access time, WAVE nodes broadcast security packets, periodic packets, and WSA packets with dissimilar transmission probabilities in all time slots. When ACK time starts, the nodes in sequence reply ACK packets to authenticate the reception of the security packets or to reserve the SCH channels with the service providers. At end of the ACK time, the nodes will tune to the explicit SCHs to achieve service transmission according to the foregoing outlet reservation.

Result and Discussion: To endorse the prioritized transmission of security packets, expected p-persistent (MP) MAC system classifies the packets transmitted on the CCH outlet into two dissimilar priorities. The event-triggered packets are confidential as the security packets with higher precedence. Seeing as the periodic packets and the WSA packets are not distributed in a real time mode, it classifies them as the packets with lower priority. In this case, the multi-priority loom can augment the delivery of event-triggered packets on CCH in a intense background.

C.TRAJECTORY BASED

(1) An Efficient Scalable Trajectory Based Forwarding Scheme for VANETs [5]:

A reactive source-based routing design i.e., SIFT. Wherein, arc is intended when needed and is just a digital map uttered in a different way, and the map is assumed to be prestored in nodes memory. During the working out phase of arc, arcs are calculated. Before the trajectory working out phase, it has been supposed that there is an entity (entity X that creates and stores an apposite digital map of the network topological environment in all the nodes of the environment. This actually starts the phase when the application layer of the source node S decides to send a message *M* to a destination *D*. *D*, possibly, does not match to a single node, but a set of nodes potentially engrossed in receiving a certain type of information. The COMPUTE arc procedure translates the destination *D* expressed as a set of geographical and topological coordinates into a mathematical equation, or a set of equations. Its presume in SIFT, that this procedure posses the appropriate mechanisms that allows it to read the digital map and to extract the mandatory information in order to calculate the equation(s) that will conform the trajectory. Once the trajectory is calculated, the COMPUTE arc course of action creates a routing layer packet P and copies into its data field the entire data field of the application message *M*.

(2) PMTR: Privacy-enhancing Multilayer Trajectory-based Routing Protocol for Vehicular ad hoc Networks [14]:

VANET-enabled vehicles with low market incursion will cause malfunction of procedure that depend on V2V communication, but bare RSU network will influence procedure that depend on vehicle to roadside (V2R) communication. There can be few connected/networked RSUs and some detached RSUs. A RSU which is detached does'nt have an Internet admission or network association to other RSUs, but it can converse with and be perhaps inhibited by a close by vehicle by means of wireless networking via the procedure. It alleged that chronological vehicular traffic figures are vacant. These may be incorporated with digital maps.

Proposed routing protocol: PMTR is a routing protocol of source where source specifies the route a message has to follow to reach the destination. It defines the route as the trajectory of cells that a message follows from source to destination. Selection of cells for a particular route is made in a mode to maximize the successful delivery rate, which is achieved by selecting cells such that the directional flow of traffic, from the source cell to the destination cell, is maximized. It includes the subsequent:

- *Layered division of area*
- *Privacy Preservation based on Cell-level Trajectory Routing*
- *Traffic Statistic*
- *Proposed Routing Protocol*

Result and Discussion: A protocol of routing that is well apt during the preliminary deployment stage of VANET where the number of (smart) vehicles as well as the number of roadside infrastructure will be partial. The protocol of routing makes use of historical vehicle traffic statistics and coarse trajectory information form vehicle to route the messages. Then protocol of routing is then compared with three altered protocols, covering a spacious range of information from users: Flooding, GeoDest and GeoTrace, and have shown that proposed protocol performs superior or equally well than those while affording better privacy or lesser overheads.

V. COMPARISON OF THESE TECHNIQUES

In this section, we present a comparison of the traffic control techniques discussed above. Tables 2 and 3 and 4 represent a summary of our study. For each technique we present the following criteria: We first start with the algorithm name, forwarded by the approach, types of messages, results and lastly discussion. Table2 states comparison of Rate Adaptation schemes Table3 states comparison of Media Access Control schemes and Table4 states comparison of Trajectory based schemes.

Table2: Comparison of Rate Adaptation scheme

Algorithm	Approach	Types of Messages	Results	Discussion
Congestion Control in Vehicular Ad Hoc Networks	Rate Adaptation	Both Periodic Messages and Event Driven Messages	avoids starvation and increases the efficiency	Highly dynamic network topology conventional mechanisms difficult to apply.
Distributed Rate Control Algorithm for VANETs	Rate Adaptation	Event Driven Messages	Number of vehicles that receive ED Msg. sent by a node (by bursts) is higher	Scenario very rare. Performance is not improved.
Congestion Control Framework for Disseminating Safety Messages in Vehicular Ad-Hoc Networks (VANETs)	Rate Adaptation	Event Driven Messages	Reducing rebroadcast redundancy in a high-density network.	Supposes to reduced the channel load in order to meet the QoS requirements
Performance Evaluation of Beacon Congestion Control Algorithms for VANETs	Rate Adaptation	Periodic Messages	A decrease in CBT throughput	The performance is insignificant when the number of intersections is small.
Congestion Control Algorithm in Vanets	Rate Adaptation	Both Periodic Messages and Event Driven Messages	Warning delay (delay of ED Msg.) is greatly lesser	Queue threshold is static. ED Msg. are totally prioritized on PER Msg.

Table3: Comparison of Media Access Control schemes

Algorithm	Approach	Types of messages	Results	Discussion
VC-MAC	Media access control	Periodic Messages	Throughput increased, and collision reduced	invent only to lead with televise scenario.
MP-MAC	Media access control	Both Periodic Messages and Event Driven Messages	High reliability of ED Msg., and collision reduced	Not suitable for Multi-hop communication.
SP-MAC	Media access control	Both Periodic Messages and Event Driven Messages	Improves the saturation throughput on CCH	Not designed for multi hop wireless hidden terminal.

Table4: Comparison of Trajectory based schemes

Algorithm	Approach	Types of messages	Results	Discussion
ESTF	Trajectory based	Periodic Messages	Scheme reduces the control overhead to zero achieves better delivery ratio	Does not require neighbor information
PMTR	Trajectory based	Both Periodic Messages and Event Driven Messages	performs better privacy or lesser overheads	Well suited during the initial deployment stage of VANET

VI. CONCLUSION

Congestion control for VANETs is a challenge and a very rigorous research topic. Throughout this paper we surveyed the most important congestion control techniques proposed to reduce congestion on VANETs, and proposed a categorization of these techniques into three classes: Rate Adaptation, Media Access Control and Trajectory based schemes. Throughout this study, we also identified a number of parameters that must be considered when elaborating a congestion control scheme. These parameters are grouped into two classes: The class of observable parameters that provide information about the state of the network, and the control parameters to control the network congestion.

REFERENCES

[1] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, “Vehicle-tovehicle communication: Fair transmit power control for safety-critical information,” IEEE Trans. Veh. Technol., vol. 58, no. 7, pp. 3684–3703, Sep. 2009.

[2] B. Kloiber, J. Härri, and T. Strang, “Dice the TX power—Improving awareness quality in VANETs by random transmit power selection,” in Proc. VNC, Seoul, South Korea, 2012, pp. 56–63.

[3] Darus, M. Y., & Bakar, K. A. (2013). Congestion control algorithm in VANETs. World Applied Sciences Journal, 21(7), 1057–1061. http://doi.org/10.5829/idosi.wasj.2013.21.7.242.

[4] M. van Eenennaam, A. van de Venis, & G. Karagiannis. (2012). Impact of IEEE 1609. 4 channel switching on the IEEE. In 2012 IFIP Wireless Days (WD) (p. 8). Dublin, Ireland.

[5] Labiod, H., Ababneh, N., & García de la Fuente, M. (2010). An Efficient Scalable Trajectory Based Forwarding Scheme for VANETs. In The IEEE International Conference on Advanced Information Networking and Applications (pp. 1–7). Perth, Australia.

[6] Taleb, Y. M., Merniz, S., Harous, S., (2017). Congestion Control Techniques In VANET: A Survey .In IEEE Conference.

[7] Shao, C., Leng, S., Zhang, Y., & Fu, H. (2014). A multipriority supported medium access control in Vehicular Ad Hoc Networks, 39, 11–13.

[8] Le, L., Baldessari, R., Salvador, P., Festag, A., & Zhang, W. (2011). Performance Evaluation of Beacon Congestion Control Algorithms for VANETs. In The IEEE Global Communications Conference (p. 6). Texas, USA.

[9] Wischhof, L., & Rohling, H. (2005). Congestion Control in Vehicular Ad Hoc Networks. In 2005 IEEE International Conference on Vehicular Electronics and Safety (pp. 1–6). Xian, China.

[10]Drigo, M., Festag, A., Baldessari, R., & Zorzi, M. (2009). Distributed Rate Control Algorithm for VANETs (DRCV) Categories and Subject Descriptors. In Proceedings of 6th ACM Workshop on VehiculAr InterNETworking (VANET) (pp. 3–4). Beijing, China.

[11] Yusof, M., Darus, B., & Bakar, K. A. (2011). Congestion Control Framework for Disseminating Safety Messages in Vehicular Ad-Hoc Networks (VANETs). International Journal of Digital Content Technology and Its Applications, 5(2), 173–180. http://doi.org/10.4156/jdcta.vol5.

[12] Fracchia, R., Meo, M., & Rossi, D. (2006). VANETs: To Beacon or not to Beacon? In 1st IEEE Workshop on Automotive Networking and Applications (p. 9). San Francisco, USA.

[13] Zhang, J., Member, S., Zhang, Q., Member, S., Jia, W., & Member, S. (2009). VC-MAC: A Cooperative MAC Protocol in Vehicular Networks. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 58(3), 1561–1571.

[14] Hsu, W. C. M., Hsieh, Y. T., (2013). A Probability Based MAC Channel Congestion Control Mechanism for VANET. In 2013 IEEE 77th Vehicular Technology Conference: VTC2013-Spring (p. 5). Dresden, Germany.

[15] Aslam, B., Amjad, F., & Zou, C. C. (2013). PMTR: Privacy-enhancing Multilayer Trajectory-based Routing Protocol for Vehicular ad hoc Networks. In 2013 IEEE Military Communications Conference PMTR: (p. 6). San Diego, USA. http://doi.org/10.1109/MILCOM.2013.154

[16] Lin, W., Li, M., Lan, K., & Hsu, C. (n.d.). Communication: a measurement study, (1), 1–13.