International Journal of Engineering & Technology, 7 (4.19) (2018) 711-719

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Survey on VANETs: Challenges and Solutions

Hassan HadiSaleh*[1], SaadTalibHasoon[2]

[1, 2]College of Information Technology, University of Babylon, Babylon, Iraq
[1]Diyala University, Diyala, Iraq
**Corresponding Author E-mail: hassan@sport.uodiyala.edu.iq*

Abstract

Vehicular Ad-hoc Network (VANET) is an advanced style and subcategory of a Mobile Ad hoc Network (MANET), the main objective of VANET's is to create an Intelligent Transport System (ITS), to reduce traffic congestion, accidents or assistance as gates to other networks such as the Internet. VANET is responsible for the communication between moving vehicles in a certain environment. A vehicle can communicate with another vehicle directly which is termed Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a Road Side Unit (RSU), identified as Vehicle-to-Infrastructure (V2I). VANET networks have now been established as reliable networks used by vehicles for communication on highways or urban environments. The goal of VANET is to help a group of vehicles to establish and maintain a network of communications between them without using any central base station. Along with benefits, there are a large number of challenges facing VANET. In this research, we present a comprehensive review of the challenges facing these networks with some of the proposed solutions, Researchers will gain best understand of VANETs challenges and research trends from the study.

Keywords: *VANET, MANET, ITS, V2V, V2I.*

1. Introduction

Currently, public and private vehicles are used daily intensively by people. The problem is that the number of deaths from road accidents has increased with increasing use of private transport. Data transfer in the VANET is done through wireless communication using IEEE 802.11p standard. Two models for communication: V2V model; that communicate with other vehicles directly or to connect to RSU equipment, referred to as V2I model [1-4]. Communication models allow sharing different types of information between vehicles, i.e. information of safety application for preventing accidents, an investigation after an accident or traffic deviation. Other types of information are the non-safety application such as passenger information, Purpose of sharing information is to offer a safety message to inform drivers of risks predictable in order to avoid accidents and save the life, or to offer enjoyable trips [4-8]. The main contributions of this paper are the introduction of the latest technology in VANET technology. A detailed study of network architecture with different topologies and network modeling is presented in this paper. The main design area in the VANET in order to correctly configure a communications network is to route packets effectively. The paper discusses VANET's Vantage Guidance algorithms and displays the limitations of these algorithms. Security and privacy issues are also addressed in the VANET environment in the paper so that the trustworthy network structure can be designed. The paper also discusses some key research areas and challenges such as congestion control, prioritization of data, overlapping across layers, and reliability. The Rest of the paper structured as follows: Section II, represents the Applications of VANET. Section III presents the Vehicular network challenges. Section IV describes Vehicular network solutions, Section V provides of the Decisions and future work. Finally, section VI, some of conclusions of the paper.

2. Applications of VANETs

1) Safe road applications.:
VANET is mostlyused to reduce the road accidents which resulted inpassenger's loss of life. These applications offer info and support the drivers by sharing information (position, intersection position, distance and speed) between vehicles and RSU for avoiding collisions with other vehicles. Using Exchanging information to detect hazardous locations. Some models of applications are given below [9-12], as shown in Fig.1.

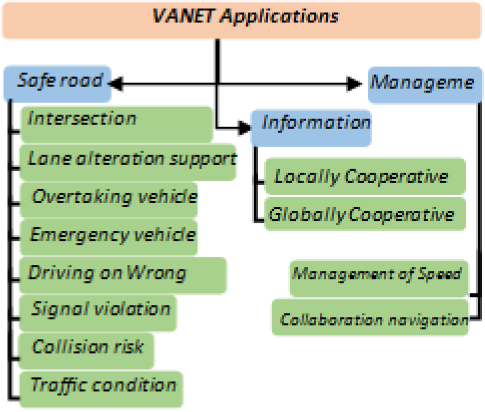

Fig. 1: VANET Applications

Intersection accident: Collision risk that came in intersections sensed through vehicles or RSUs.

Lane alteration support: Side impact danger of vehicles that changing path is reduced with an unseeing area.

Overtaking vehicle: The risk of third-party exposure to prevent collisions between vehicles in a bypass mode, where a single vehicle, for example a vehicle1 ready to overtake a vehicle 3, whereas additional, vehicle 2 already achieve passing operation on vehicle 3. Crash between 1 and 2 is prohibited when 2 notifies 1 to stay its passing process.

Emergency vehicle: A dynamic emergency vehicle, i.e., a police vehicle, ambulance, can inform adjacent vehicles to empty or leave the required emergency lane. Such useful messages can be replayed by other vehicles or RSUs.

Driving on Wrong way:A car found to be driving in the wrong way, for example, a prohibited address, denotes to this state to other vehicles and RSUs.

Traffic condition:Any rapid transit development detected by vehicles, learns others (vehicles and RSUs about the state).

Signal violation: RSU detect a violation. Information transmitted through a RSUs to all neighborhood.

Collision risk: RSU detects any collision between vehicles that don't have facility to interconnect. RSU broadcast information towards all cars in neighborhood.

2) Management of efficient Traffic applications:

These applications concentrate on improving traffic flow for the vehicles, speed management and offer maps update. Some models of applications are in [8-9].

- Management of Speed: the Goal to support the driver to manage speeding and to prevent unnecessary stopping. Controlling speed limit notification.
- Collaboration navigation: This type used to increase efficiency of traffic by managing vehicles steering over the support between V2V and RSUs. Traffic Information and route, are two case of this type.

3) Information and Entertainment Applications:

a) Locally Cooperative services: This type concentrate on information obtained from locally services such as media downloading and e commerce [9], [10], and [13].

b) Globally Cooperative services: It concentrate on information obtained from global services such as Internet, which include financial facilities, parking management, which concentration on data updates [9], [10], and [13].

3. Vehicular network challenges

Previous section debate some of applications that use V2V, V2I communication. Applications domain, extend from information and entertainment application, such as downloading media to safety applications, like a cooperative awareness of drive assist, require a variety of requirements for support vehicle network support techniques. These different requests lead to no of challenges. Although there is fully research in the VANET network, there are still many areas to consider. Due to the changing nature of Vehicular networks and demanding requirements, there are a number of problems. This paper discusses some of essential challenges areas as is the case. However, it should be regarded that the VANET research requests are not restricted to these fields only. This section describes challenges difficulties as shown in Fig. 2.

A.Addressing: Some of applications require address linking to the physical site of the vehicle, making navigation and managing "geo-addresses" very hard.

B. Risk analysis: is used to detect threats and potential attacks in VANET communication. Solutions have been proposed to avoid such attacks, but there are still models of the behavior of the attackers misplaced.

C. Data Trust and verification: Data trust is more valuable than the guarantee of nodes that join that data. Trust and verification of data offer protection means to VANET applications to support and ensure the information is confidential and the receiver may validate information integrity in order to the protection of a network from intrusions and impersonation security threats [16]. Cryptosystems is useful in this application but the central difficulty is incorporated with the cost that is added by using of a public key system [17], [44].

D. Privacy, Secrecy, and responsibility: Hosting data from different vehicles in the network rather from another network should be trusted in some way by the entity that created the information. In the same time, privacy is an elementary right that is must be protected, via laws. Privacy can be given by secrecy vehicle identifications. Principal objections here is to develop solution that capable to maintain tradeoff among Privacy, Secrecy, and responsibility while network should confess transferred information and references to specific governments.

E.Localization Security: Is a flexible and reliable denial of service (DoS) tool allied to vehicle network protection against attackers who want to knowingly retrieve location.

F.Delay constraints: Time and place are usually essential in the process of transmitting data packets by VANETs applications; the Main task in planning VANET protocols is to offer an appropriate performance of delay under the restrictions of speeds, changeable connectivity, and topological variations. The network has smallest delay for data transfer, fewer retransmissions, and long connectivity time offer specific Quality of Service (QoS) confirmed to users.

G. Packets congestion control and prioritization: the impact of the packets carrying traffic information (i.e. efficiency and/or safety) is greater and faster than others. Most of research accomplishments have concentrated on how to offer uppermost importance to emergency kind of data. When an emergency happens.

H. Cross-layering and Reliability: Due to the wireless communication nature of network, a route may break abruptly. A reliable transport service should therefore be provided as far as on the head ofthe unreliable network. Designinga suitable cross-layer protocol involvingtransport and routing layer in VANETs is being beneficial because it boosts applications [12, 14].

Vehicular network challenges
Addressing
Risk analysis
Data Trust
Privacy
Secure Localization
Efficient Routing
Delay constraints
Packets congestion
Reliability

Fig. 2: VANET challenges

4. Vehicular Network Solutions

Some solutions to the previous challenges.

A. Addressing: Packets transferred via VANET need specific address and rout topographies. In [18], packets were typically sent behind topological prefixes and therefore can't be adjusted to track topographical routing. In [19] Identify destination addresses from GPS positioning. Address of GPS could be characterized by using: Polygons, like a circle radius, any node located in the geographical area might receiving a message, in [19], [20], Three keys are capable to integrate physical location in an Internet scheme that depend on logical processing. These keys are:

i. Application layer key for addressing: by using Domain Name System (DNS) protocol to locate position. DNS stretched databases by using geographic information, DNS contains the complete directory to access the IP address level of each base station and its exposure zone represented by a circle. More than one domain is included where the first domain represents geographic information, other domain represents states, third denotes to provinces and last domain represents geographical organizes. In a similar way geographic address is determined as classic address, using IP addresses of base stations that covering specific area. Two options were distinguished. first, group of unicast messages is directed to IP addresses resumed by DNS. IP address placed in given area match the base station, then base station sent message to all communicating nodes with it, using filter of application layer. Second, all stations situated in geographic area joined the multicast group temporary for area that geographically identified in message. Messages that must be sent to the region on multicast mode using this address [20].

ii. Unicast routing key based GPS: The keys related to the geographic places are stated in following:

a) Geometric Routing Scheme (GEO) [19]: uses the destination information of polygonal geographic in GPS header. GEO using a simulated net, contained of GPS facilities, by applying GPS positions in routing over layered onto existing IP network.

b) Geographical Positioning Extension for IPv6 (GPIPv6) [21]: defined for geographical data distribution in IPv6 protocol. It requires the specification of GPIP source and destination, it encompassed of signing the position of geographically source and destination.

c) Using unicast prefixes to target multicast group members [22]: Extension to IPv6 architecture is define to permit for unicast-prefix based sharing of multicast addresses. Extension can be used for objective multicast memberships within specific area.

iii. GPS-Multicast Addressing key: this method GPS Multicast Routing Scheme (GPSM) is uses. Here each fragment (smallest geographic area) is charted to a multicast address area that can have a geographic address. Whereas a partition (large area) cover more than one atom. A partition can represent (state, county, town), the idea of the protocol is to estimate polygon address of least partition, which is contained in, and through the use of the multicast address equal to partition as IP address of this message [23].

B. Risk analysis in VANETs, It has not been investigated widely yet. Multiple frequently cited a research about invader abilities in VANETs [23], it defines the work through German idea [24]. security project used is flexible, permitting to participate earlier found attacks into deliberate four main attack features:

- Interface Attacks;
- Running the Software on RSUs and OBUs Attacks;
- Vehicles Sensor inputs to different processing units;
- Infrastructure Attacks behindhand contact networks, such as vehicle traffic, manufacturer's authorities, and certification .In[25], two ways defined to improve security:

- Conduct local tests by comparing information received by data sensor and evaluating received information from other source of event;
- Perform authorizations on nodes, especially on RSU.

C. data Trust and verification, ideas of security could be used are categorized to two ideas (proactive, reactive) [23].

1) Proactive concept: which is considered a best encouraging candidate for transportation safety applications in VANETs, this kind is divided into three categories:

- Engaged messages arise in two domains: digitally messages signed with and without permits. The first is easy to arrange and usage, while other provides a further secure, but with additional compound connection. Identical answers established in [24-27].
- The proprietary system design: Design has non generic protocols, and custom devices. Earlier use of non-generic protocol to succeed access limits to the nodes that don't use this protocols. Later a modified devices uses to accomplish an analogous objective. Note the keys don't evade any enemy from damage affected, so a goal is to raise a requisite power that the attacker must exhaust to access to system.
- Tamper resistant devices: until while safeguarding external contact portion of application, it is improbable to guarantee the system inside a car is free for generation, for example, needless cautions of accidents. answer for this problem is using of tamper resistant devices. Some of examples explained in [28, 30].

2) Reactive security: consist of three approaches that based on (Anomaly, Signature and Context). They associate received information with system information from explanations in system procedure [29] and [31].

- Signature based approach: intrusion discovery by comparing identified signatures of attacks with network traffic to determine attacker of the system.
- Anomaly approach: intruder detected compares one derived from normal process performance by received information. In this solution we must determine the behavior of the available system communication [30].
- Context approach: in this approach the information collected from any vehicles available on area, to create self-governing view of existing state and environments. When data received by the vehicle, the parameters compared with related states and situation, e.g., information estimated and Position with it's regarding the state and environments to discover any intruder. Context based kinds are:

❖ Verification of Position Information purposes to avoid an invader of acting to be at unreasonable states.

❖ Time verification compares synchronized clock of a vehicle with provided information from GPS, with the time of messages that received.

Applications that depend on verification solution associates context of application with an analogous are known to a vehicle. Examples of Application Context verification is in [32-34].

D. Privacy, Secrecy, and responsibility

Privacy and Anonymity: Anonymity must ensure that encrypted messages do not allow sender identification. Additionally, it is difficult to connect more than two. Secrecy and adaptive privacy: privacy is an adaptive concept is presented in [35] and [36]. It's a good tool that should allow users to specify the privacy they want. The higher level of privacy necessities generally increases communication and redundant computing. User may need using a different level of privacy subject on whether is connecting through private server or public server. The trust strategies contain, complete trust in which user trusted in both servers, incomplete trust, where users trust one server and nothing trust where neither of these servers users is trusted by users.

E. Responsibility: This challenge is stated in [16], but without solutions delivered. Most of the secrecy solutions that stated in [36] could fulfill the responsibility by adjusting the privacy degree of user.

F. Secure Localization**:** Numerous keys are proposed [35-39]. Where most vehicles have a GPS in their receiver, which can record location at every period and offers these information to another node in network in a reliable way. Many solutions were suggested in literature. [38] Suggests Tamper-proof GPS system, each vehicle have tamper-proof GPS receiver, the position can be registered at all times and provided to new node in network in real method. The problem is that the availability is restricted in urban situations, e.g., GPS receiver's problem on tunnels, bridges. Moreover, GPS based systems are susceptible to numerous attack, such as physical attacks, spoofing, and blocking. Inspection the location of the vehicle cooperating with the roadside infrastructure and utilizing the multi-iteration and the distance limits [38]. Using Distance hopping to guarantee that the in-between nodes distance is not greater than precise value. Multi-iteration means similar process was used in a number of dimensions. One of the processes that use verifiers to create positions is suitable in [39], propose a solution based on challenge and response that demand verifiers. Nodes are set on private locations defining a suitable distance for each verifier. Verifier are set in each circle. It requests from vehicles to refer hers place. Then, verifiers refer to a communication link challenge in vehicles. When vehicle receives the task has to reply through ultrasounds. When a response arrives at a specified time, it is concluded that the vehicle is within Area (R). Alternative challenge reply system includes using of logic response of beacons [40], which comprises consist from acceptor and rejecter nodes. Acceptor spreading completed region (R), whereas rejecters form a closed ring rounded receptors. If the vehicle sends the beacon, the verifier receives a message determine whether the position of vehicle is satisfactory. If themessagearrive a rejecter then the vehicle cannot be staying in region (R). And if it reaches to the others, it confirms to be located within region (R). In [41, 42] new notion of Position Cheating Detection System (PCDS) is come in. In this method suitable sensor was used to sense cheated information of position. Two sensors classes can be used to verify the position. First, Autonomous Sensors, The sensor results in the whole confidence ratings of adjacent vehicles freely. Second, Cooperative devices, which cooperates with other vehicles nearby the control adjacent node. In both devices, use network layer provided information. This leads to no additional infrastructure is required, since only network vehicles are involved. Plausibility can be used as an alternative check. Secure Location Verification (SLV) and the answer established for Routing Position Based (RPB) are two examples of the plausibility checks. In [43], SLV was suggested to sense and avoid the position attacks performed by distance bounding. On the other hand, [44] develop a Position Based Routing (PBR) secure localization solution. PBR provides an efficient and scalable unicast. Such unicast is retransmitted in large scale VANETs. Threefeatures are used to construct the PBR, these are: forwarding, location service and beaconing. When an emerging vehicle wants to identify the location of another vehicle which is not found in its built table, location service can be used. This occurs when the vehicle that generates the message sends a location query that contains sequence number, hop bound and ID. The node that receiving a message and not intended to search, resend site query message. While searched node returns a location reply message with its timestamp and current location. Originating node updates location table when it receives the location reply message. for securing PBR messages, i.e., location reply and query for location, information of time and location fields of packet using as inputs for every received note to pass specific plausibility checks. The message is discarded when checks fail. Else, verification continues. At First certificate is validated except if it was validated in previous. If passes the verification then verify digital signature. If all steps passes, then message is further processed, else it discarded [46].

G. Delay constraints, this part classified every delay protocol by taking suitable steps depending on the layers.

1) Application Layer Approach: Delay bounds are necessary at the standards of the requested layer because it is required to handle emergency important warning messages. Constantly, broadcasting these messages inside the artificial zone is being possible. To combat the transmission problem, the requests are usually requiring a strong routing mechanism or devices that avoid repeated re-broadcasts that can slow the spread of messages. In [47] an emerging vehicular safety application, an examination of highway cooperative collision avoidance (CCA) protocol was presented. This protocol is involving a model for drivers to evaluate the emergency level and suitable caution hint. Always, Critical posts were broadcast by a directed aware transmitted scheme with implied salutations. Conclusion of authors, specific setting and limitation parameters should planned in an application mode. For example, CCA messages would be forwarded toward the affected vehicles directions wherever they are presented. In [48], a delay control protocol called transmission range was described. This protocol considered as a fast broadcast in which the permission is given to the sender to guess the transmission limitations before transfer the packets. The delay control protocol is restricting the amount of messages exchanging in network, so, it decreases the whole transmission time. In [50] was studied packet flows to support QoS for multimedia applications (video, data packets and audio) in VANETS. QoS can be supported by IEEE 802.11e in the MAC layer. This standard assigns a diverse import value for each packet flow type. Through a detailed experimental analysis, authors showed that 802.11e is primarily proper for MANETs and not applicable for VANETs. According to the fact that the typical may not yield vehicle traffic, link quality, and multi-hop communication effect into account - which stimulates the need for cross-layer design among MAC and network layers. They present a DeReHQ algorithm which transfers packets over routes with greatest link accuracy, minimum no of hops, and link delay is within the desired threshold [50].

2) Network Layer Approaches: delay limitations can also be embedded into in network layer protocols. Design of protocols with delay characteristics and delay of the warranty is problematic since the vehicles have high mobility. Other description was a few location based protocols are exist in D-Greedy & D-MinCost [52], VADD [53], and PROMPT [54].

3) PROMPT and VADD make delay estimate through the track choice, D Greedy& D-Min Cost worked on statistical track-info by using them in routing the packets over the minimum end to end delay paths. It considers simply those tracks that are within a limited delay. An important challenge is a delay estimation for each track before a choice amongst obtainable ones is make. VADD worked on using the available loaded statistical information like speed and density of vehicles to estimate the track delay. PROMPT, used an existent time packet statistics in the looking for tiniest delay path. Likewise, DeReQ protocol [55] attempts to achieve its objectives timeliness and reliability through finding a path that is most dependable and has delay within a permissible best bound. Reliability estimation, DeReQ used the density of traffic road, relevant speeds of vehicle, and traffic flow. Alongside with location based approaches, they are including certain topology based protocols using link stability through approximating the routes lifetime. Mechanism of estimation used by sender to choice best convenient route to transfer the packets. The relay points send path request for new route prior to breaking the current path [55]. These methods have a significant impact on end-to-end delay by packets.

4) MAC Layer Approaches: The effectiveness of the IEEE 802.11p modification for safety applications, requiring low latency, real time communication, and reliable was studied in [56]. It experiments that CSMA/CA technique of 802.11p standard does not assure channel access prior to the limited deadline thus, it provides poor performance. Authors of [56] suggested a self-organizing time division multiple access (STDMA) method. STDMA is a distributed system in which every vehicle directs its specific slot job depending on its location and the neighbor’s information. The method aids in estimating the channel access delay, so it will be appropriate for real-time VANETs. Some researchers have used multiple directional antennas to deliver packets quickly. For instance, RPB-MAC protocol [57] decreases the overload of the control message and ensures minimal delay in channel access through using multiple antennas. A pair of communicational channels was used allocated with a directional antenna, all together assigned to a group of vehicles according to their possessions relative to the source vehicle. Because cars located in multiple directions relate to the use of multiple antennas, that caused the channel collisions number to get reduced. In addition, transmission power was adjusted adaptively to sustain its neighbor's communication.

5) Physical Layer: In [58] Accident Warning System (IWS) utilizes straight wireless communication to transmit a range of packets containing traffic accident reports, text messages, JPEG images, and so on. Divide applications into three diverse categories and identification necessities imposed through applications in each group. These necessities controlled by applying two dissimilar frequencies. First: long range frequency

represent channels retention; short-range frequency representing packets transmissions. Power adaptation is another method that researchers used to achieve a small delay in the node to node. Several papers are discuss Transmitting power adaptation, see e.g., [59], [60] and [61]. Only [62] will be discussed, the vehicle is able to screen channel environments through computing overhead ordered statistics and numbers. Vehicle records the delivery of successful packets sent by adjacent nodes using the same radio channel that is inside the broadcast and get the distance of the reception vehicle. By calculating plus identifying packets that had been positively received, the reception vehicle is able to identify unsuccessfully the packets plus deciding the status of the network, i.e., the middling rate plus packets rate that had not been positively delivered. From above analysis, the recipient node is similarly able to calculate the least amount of nodes using similar radio channel. Then the calculated channel circumstances used to acclimate its broadcast power consequently. The beaconing adapted tools defined in [63] it did not distinguish amongst the periodic and occurrence derived messages that transferred through beingIEEE802.11p control channel. In [64], another couple adaptations algorithms for transmission's power were discussed to monitor the beaconing capacity. Emergency message Dissemination for Vehicular environments (EMDV) and Distributed Fair Power Adjustments for Vehicular environments (D-FPAV). The D-FPAV is a divided the control strategies of transport power that offers operational transportation for emergency event-driven messages whereas preserving equality intended for periodic beacon messages. Every node evaluated the consumption rate of the receiving channel that has been evaluated since the last beacon was sent. This amount computed from statistics in connection layer or else through the statistics of the network layer. Every beacon holds this value. Furthermore, the node preserves the aimed channel usage ratio. If the receiver channels usages less than the target value, the conveyed power will be improved by one. If the usage rate for the receiving channel is higher, the transmitted power would be reduced by the same amount. Broadcast power will not be switched while the amounts are exactly the same. Additionally, D-FPAV protocol lets you prioritize occasions based messages via periodic messages. The lowest distribution of power levels for a vehicle is computed via selecting minimum detected rate for the power allocation stages between receiving's beacons. EMDV protocol using dispute approach that supports effective and fast distribution of warnings inside a physical area supporting D-FPAV. In EMDV, you choose the basis vehicle which desires to direct a warning (crisis) message to the convey node as long as probable and having a high response probability. Upon positive reception, the relay node resends warning messages. Thus, if receiving a packet failed in the identified convey node, different vehicles that are receiving the messages would be considered as a potential convey node. This node delayed for a specified time, i.e., rebroadcast message only if no replay is heard rebroadcasts throughout waiting period and retransmission delay timer. Also, this algorithm is able to differentiate between periodic and event driven messages. Research [65], EMDV and D-FPAV used as base protocols. EMDV improved by, modifying the re-broadcasting waiting timer when every new receives of desired information that had been re-broadcast. The delay timer was adjusted in a way to result in a constant geographical allocation of the rebroadcasting conveys. This would be done by reassessing the delay timer through considering the distance to nearest motor – cars of relay vehicles. Those who can re-transmit same information. On the other hand, the D-FPAV protocol was improved by adapting algorithm in a technique rather than dealing out with the traditional usage from a single edge area. Every vehicle wants to operate the usage data expected beacon from couple edge areas, front plus behind vehicle lengthwise the route. In this circumstance, a compression would be between target rate and actual rate. The later computing computed by linear interpolations of the utilization rate for the receiving channel and distant beacons in the behind and front vehicle. In [66] transmission power was adjusted adaptively to adjust modifications in neighbors. If no of neighbor's drops below threshold, the power will be amplified. Beside, whenever the no go beyond another threshold, power would be reduced consequently. A possible obstacle, thresholds are not reflecting diverse traffic circumstances and value of road sections. In [67] DB-DIPC Suggested techniques for adapting power to vehicle networks that rely on local information obtained through the intervallic conversation of beacon messages between neighbors. In [55] LOADPOW is using information of traffic load routing procedure to regulate re-transmitting earlier packets and send them through medium entrance layer. Adapting and distributing such algorithms is possible. Thus, a need for extra study to understand influence of adaptation on altered performance metrics.

H.Prioritization: the data packets during an emergency occurrence causes the channel usage to be reduced due to vast transmission of messages. In such cases a simple approach that relies on adapting a number of protocols, is simply to drop the lowest primacy packets. Other protocols are trying to offer suitable overcrowding control tools. Therefore, packets transmission rate for less priority would be adjusted at lower rate. In [60], Vehicle Collision Warning Communication (VCWC) is a model of supportive accident cautionary system that supported by node-to-node communication. The objectives in providing lower latency message broadcasting in the preliminary level of alternative event. Packets blocking problem was handled through a rate variation scheme that sets altered priority levels for multiple packets depending on application requirements. When the node holds an emergency message (backlogged), it signals a busy tone outside the range that would be sensed by others vehicles placed between couple hops. Motor cars has delay messages of low priority comply channel accessibility when full tone sign is detected. Additionally, bandwidth usage was enhanced by blocking various warning messages related to same incident. In [68] the channel congestion control studied in 802.11p standard plus proposed on packets in CCH (control channel) must be ordered. Protection messages must require an upper priority than control or background messages, like a periodic beacon or welcome messages. It provides mechanisms to control different congestions by manipulating the MAC queue. Beside, core idea is giving complete importance (priority) to safety messages by handling (for example, freezing) MAC queues of the lesser importance, or dynamically retaining a portion of the bandwidth for high importance with adaptive quality of service parameters. In [69], similar systems based on 802.11e standard were suggested toward offering upper importance to crisis messages. In [70], a control mechanism pulse had been suggested to deliver main firm for urgent messages. Depending on that method, when emergency occasion is detected, vehicles would establish an unsystematic back off timer whose value according to the situation of emergency. Once the back off timers is finished, vehicle will start transferring pulses in control channel, emergency packet is sent to data channel, just after beginning to sending the pulses. When a pulse is detected in control channel by the node at one time, it cancels transmission operation to release both channels. This operation provides a strict priority to emergency messages.

I. Reliability and cross-layers among layers of conveyance and the network, some research activities available in the design of cross-layer protocols that extend among transportation and network layers. This layered design is driven by support for real – actual – time plus combination applications that involve node-to-node reliable connection to QoS constraints. Cross-Layered strategies similarly are helping to avoid congestion. Because of repeated disturbances in routes, transportation in layer protocols of MANETs [64], do not apply directly to VANET. One must take advantage of the info from the network layer to adjust packet broadcasting in the transportation layer to adjust the dynamic network topology in VANET networks. First, we deliberate a number of tasks in the presence of conveyance layer protocols in

VANETs. Since Transmission Control Protocol (TCP) was absolute common transportation protocol, we do not discuss TCP protocol in VANETs. TCP was formerly intended to wire networks with suitable data transfer capacity. Still, the basic features of mobile networks like dynamic topology and changeable wireless transmission were exact dissimilar from wired networks. Numerous research into the influence of those characteristics. On TCP actions have shown that they provide a weak output in vary hop- ad- hoc networks [71]. That week action is mostly because of the congestion control and traditional flow technique popularized in TCP. For instance, TCP infers communication errors as an overcrowding mode so that reduces the transfer speed. In [56], writers' dispute that powerful routing protocols could be castoff to report the TCP difficulties in dealing with road interruptions in VANET networks. Authors studied the TCP optimization and geo-routing parameters to deal with high-speed vehicle. In the monitoring network, the high traffic effect is shown on important TCP plus UDP system parameters like welcome message interchange rate. Then they offered a schematic scheme where the duration of the hello rest on the speed of the vehicle: I = R* K * S, where S is the speed, K is a tunable parameter, R represents the range of transmission and I is the interval.

Table 1: VANET challenges and conclusions

Addressing	Three solutions identified: the most promising but also more complex solution, which offers IP (routing and address) to dealing with GPS. Whereas several keys have suggested, extra research and consolidation activities are needed for success.
Risk	A small scale research have been done. From these studies, we can conclude that the position forging attack is a major weakness of the system.
data Trust and verification	Proactive concept of security has been extensively researched. Further research should be conducted to combat interfere (tamper) in vehicle (sense redundant accident cautions), desires more researches. Reactive concepts of security considered in less studies. Further verification context effort is needed, since vehicle has ability to achieve detection by connecting the information received to state and environment parameters with information.
Privacy, Secrecy, and responsibility	Responsibility, privacy widely investigated. However, an open range is adaptive privacy and Secrecy, where the users are permitted to choice privacy that request to have. Effective responsibility explanations are not delivered. An important effort in this range is required.
Secure Localize	It considered that the best and most effective solution to DOS attacks is secure localization. It need an extra effort in the range of tamper proof GPS and using of reasonable checking to evade attacks.
Delay constraints	The major problematic task with designing a better protocol is to afford well delay performance underneath limitations of extreme speeds of vehicles, fast topological changes, and unreliable connectivity. In this unit, many methods have been discussed which include delays limitations on several layers. Though, realizing that individuals replies nodes. Example, rising the variety of transmissions, reduces the amount of hops, this can decrease node to node transmission delay. But, increasing variety of transmission would cause extra MAC conflict delay. Offering general system optimization, upcoming answers should focus on multilayered protocols that balance conflicting issues from different layers in order to reduce node-to-node delays.
Prioritization	More efforts must be made to increase the effectiveness of IEEE 802.11p and 802.11e standards. For example, protocols across layers that work in more than one layer to offer priorities between multiple pests and different applications. Moreover, the development of effective schedule methods that assist the communication of packets to diverse priorities was a major concern for upcoming applications of VANET.
Reliability and cross-layers	Most of the previous work focuses primarily continuously upon methods that required a unicast routing. Because many applications like safety applications always requires transmission of radio and communications, obviously a need for different methods that are not build on traditional transportation protocols. It is complicated and perplexes in case of locating protocols where migration nodes (relay) in such approaches do not retain any information about the situation. The cross-layered design has a favorable upcoming in delivering operative protocols to exceed congestion and interconnect problems.

J. Experiment shows that transport rate for equally TCP and UDP is higher when used with the adaptive system. The writers also advanced a new delivery plan outside the system. VTP [72-74] relies on a location-based directive like PBR [73-75] to deal with impermanent network segments which disconnect endwise communication plus origin packet damage. The prim approach was to take advantage of statistical path features of fault and overcrowding controller. VTP avoids pointless reductions in communication rate according to loss of non-congestion packets like routing faults via loopback from nearest vehicles. The middle nodes calculate the lowest bandwidth available nearby and re-feed the info to the sender (through piggybacking link). To compute the bandwidth delay the sender node will use the information that calculated by the intermediate node and use it to regularize the bath quality. VTP offers connection/ crash conditions to handle frequent interruptions. The sender every so often is sending a checking message to send its packets whenever an immigrant's node is available.

5. Conclusions

The main contributions of this paper are to present state of the art in VANET technology. This paper presented an overview and tutorial of various issues in VANET. Various types of research challenges are highlighted in context of vehicular communication. Research challenges and areas of interest in vehicular communication were discussed. Table 1 presented all challenges discussed in the research and conclusions.

6. Future Work

Vehicle networks is a assisting technology in supporting many applications that differ from worldwide Internet facilities besides applications founded to activate highway safety This research provides review for the recent major research challenges associated with vehicle networks, many solutions to solve the problems were defined. Below a challenges list plus recommendation for future works:

1) Addressing: The main encouraging, as well as furthermost complex, is the family of geographic addresses that extend IP routing plus IP addresses to handle GPS addresses. Whereas many outcomes have been proposed accompanied with group, further more to success a need for actions and regulation occurred.

2) Data Trust and verification: Proactive confidence has been discussed in the emphasis on data and the concept of security verification on a large scale. On the other hand, interfere solidity hardware that is in the vehicle to discover preventable accident cautions, will need extra researches. Concept of interactive security has been studied on a lesser measure. Further work needed in context verification, where vehicle is capable of achieving intrusion discovery system by comparing information received about parameters related to situation and environment with available information.

3) Anonymity and privacy: Widely investigated however, the exposed area is adaptive privacy and anonymity, allowing users to choose the privacy they wish to receive.

4) Delay constraints: The main challenge in designing the protocols is to achieve a valuable enhancement in the delay under high vehicle speed limitations, rapid topological changes, and unreliable communication. This type of challenge, we discussed many ways involving delay limitations in different layers. To provide total system optimization, the future subjected solutions should constraint on multilayered protocols that equilibrium of inconsistent issues from different layers in order to reduce end-to-end delays.

5) Prioritization: New researches such as 802.11e and IEEE 802.11p provided packets instructions. While there are some researches cared about the adoption of those standards, more efforts should be made to increase the effectiveness of these standards. For example, protocols across layers that works in multiple layers to schedule priorities among diverse pests and multiple applications. Also, development of effective scheduling approaches that allows packets transportations to different priorities is main issue of future applications.

6) Reliability: broadcasting or what it called geo-casting usually needs safety and other application, thus new methods that does not depend on transportation protocols is required. Another challenge situation where geo-casting protocols is used. In this case, Migration nodes do not maintain information about the situation.

References

[1] Olariu S, Weigle MC. Vehicular networks: from theory to practice. 1st ed. Chapman&Hall/CRC; 2009.

[2] Saif Al-Sultan, Moath M.Al-Doori, Ali H. Al-Bayatti and Hussien Zedan,"A comprehensive survey on vehicular Ad Hoc network", Journal of Network and Computer Applications, Elsevier, vol. 37, pp.380-392, January 2013.

[3] Marwa Altayeb and Imad Mahgoub "A Survey of Vehicular Ad hoc Networks Routing Protocols" International Journal of Innovation and Applied Studies, ISSR Journals, Vol. 3 No. 3, pp. 829-846, July 2013.

[4] Mr. Bhagirath Patel, Ms. Khushbu Shah "A Survey on Vehicular Ad hoc Networks," IOSR Journal of Computer Engineering (IOSR-JCE) Vol. 15, Issue 4, PP 34-42, (Nov. - Dec. 2013).

[5] Moustafa H, Zhang Y. Vehicular networks: techniques, standards, and applications.CRC Press; 2009.

[6] Jiang D, Taliwal V, Meier A, Holfelder W, Herrtwich R. Design of 5.9 Ghz dsrc-basedvehicular safety communication. IEEE Wireless Communications 2006;13(5):36–43 .

[7] R. Thenmozhi , Yusuf H., "Survey on Collision Avoidance System in VANET", INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT, Vol 3 Issue 4, 2014.

[8] M. L. Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A Survey," IEEE Commun. Surveys Tutorials, vol. 10, no. 2, pp. 88–105, 2nd Quarter 2008.

[9] C2C-CC, "Car to Car Communication Consortium Manifesto: Overview Overview of the C2C-CC System," Car to Car Communication Consortium, Tech. Rep. Version 1.1, 2007.

[10] ETSITR102638, Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Definition, ETSI Std. ETSI ITS Specification TR 102 638 version 1.1.1, June 2009.

[11] ITS JPO, "Vehicle safety applications," US DOT IntelliDrive(sm) Project - ITS Joint Program Office, Tech. Rep., 2008.

[12] SAFESPOT D8.4.4, "Use cases, functional specifications and safety margin applications for the SAFESPOT Project," IST Safespot Project, Tech. Rep. Safespot IST-4-026963-IP deliverable D8.4.4, 2008, pp. 154.

[13] PREDRIVE D4.1, "Detailed description of selected use cases and corresponding technical requirements," IST PreDrive C2X project, Tech. Rep. PreDrive C2X deliverable D4.1, 2008.

[14] VSC, "Final Report," US DOT, Vehicle Safety Communications Project DOT HS 810 591, April 2006.

[15] VSC-A, "Final Report," US DOT, Vehicle Safety Communications Applications (VSC-A) Project DOT HS 810 073, 2009 January 2009.

[16] M. Raya and P. Papadimitratos and J.-P. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8–15, October 2006.

[17] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network (Special Issue on Net Security), vol. 13, no. 6, 1999.

[18] R. Baldessari, A. Festag, and J. Abeille, "NEMO meets VANET: A Deployability Analysis of Network Mobility in Vehicular Communication," in 7th International Conference on ITS Telecommunications (ITST '07). ITST '07, 2007.

[19] T. Imielinski and J. Navas, "GPS-Based Addressing and Routing," IETF RFC 2009, pp. 1–27, November 1996.

[20] J. Navas and T. Imielinski, "GeoCast Geographic Addressing Routing," in Proc. ACM Mobicom. ACM, 1997, pp. 66–76.

[21] J. Vare and J. Syrjarinne and K.-S. Virtanen, "Geographical positioning extension for IPv6," in Proc. International Conference on Networking (ICN 2004). ICN 2004, 2004.

[22] B. Haberman and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses," IETF RFC 3306, August 2002.

[23] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmuller, "Attacks on Inter Vehicle Communication Systems - an Analysis," in 3rd International Workshop on Intelligent Transportation (WIT 2006). WIT 2006, 2006.

[24] Website, "Network on Wheels," http://www.network-on-wheels.de/about.html.

[25] B. Schneier, "Attack trees: Modeling security threats," Dr. Dobb's Journal, December 1999.

[26] T. Leinm¨uller and E. Schoch and C. Maih¨ofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," in Proceedings of 4th Annual Conference on Wireless Ondemand Network Systems and Services. 2007.

[27] M. Raya and J. P. Hubaux, "The Security of Vehicular Ad Hoc Network," in Proc. 3rd ACM workshop on Security of ad hoc and sensor networks (SASN 2005). (ACM SASN 2005), 2005.

[28] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Network," Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, pp. 39–68, 2007.

[29] M. Gerlach and A. Festag and T. Leinm¨uller and G. Goldacker and and C. Harsch, “Security Architecture for Vehicular Communication,” in Proc. Fourth Workshop on Intelligent Transportation Systems (WIT). WIT 2007, 2007, Germany.

[30] P. Papadimitratos and L. Buttyan and T. Holczer and E. Schoch and J. Freudiger and M. Raya and Z. Ma and F. Kargl and A. Kung and J.-P. Hubaux, “Secure Vehicular Communications: Design and Architecture,” IEEE Commun. Mag., vol. 46, no. Issue 11, November 2008.

[31] D. Schellekens, B. Wyseur, and B. Preneel, “Remote Attestation on Legacy Operating Systems With Trusted Platform Modules,” in Proc. First International Workshop on Run Time Enforcement for Mobile and Distributed Systems (REM 2007). REM 2007, 2007, pp. 1–13.

[32] P. Golle, D. Greene, and J. Staddon, “Detecting and Correcting Malicious Data in VANETs,” in Proc. First ACM Workshop on Vehicular Ad Hoc Networks (VANET ’04). ACM, 2004.

[33] J.-P Hubaux and M. Raya and P. Papadimitratos and V. Gligor, “On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks,” in Proc. IEEE Infocom 2008, 2008.

[34] Jose Maria de Fuentes, Lorena Gonzalez Manzano, Ana Isabel Gonzalez-Tablas and Jorge Blasco “Security Models in Vehicular Ad-hoc Networks: A Survey” IETE Technical Review, Taylor & Francis, Volume 31, Issue 1, pages 47-64, 20 May 2014.

[35] Venkatesh, A.Indra and R Murali “Routing Protocols for Vehicular Adhoc Networks (VANETs): A Review”, Journal of Emerging Trends in Computing and Information Sciences, Vol. 5, No. 1, January 2014.

[36] Shilpi Dhankhar and Shilpy Agrawal, "VANETs: A Survey on Routing Protocols and Issues," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), vol. 3, no. 6, pp. 13427-13435, 2014.

[37] Moumena Chaqfeh, Abderrahmane Lakas, and Imad Jawhar, "A survey on data dissemination in vehicular ad hoc networks," Vehicular Communications, Elsevier, vol. 1, no. 4, pp. 214-225, October 2014.

[38] Hassan Hadi Saleh, “Increasing Security for Cloud Computing By Steganography in Image Edges”, Al-Mustansiriyah Journal of Science, Vol. 27, No 4, 2016, pp.83 -87.

[39] Hassan Hadi Saleh, Soukaena Hassan, “CRITICAL AND IMPORTANT FACTORS RELATED WITH ENHANCING WIRELESS OMMUNICATION USING MIMO TECHNOLOGY”, Diyala Journal of Engineering Sciences, Vol. 08, No. 01, March 2015.

[40] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, “Adaptive Privacy-Preserving Authentication in Vehicular Networks,” in Proc. First International on Communications and Networking in China (ChinaCom ’06). ChinaCom ’06, October 2006.

[41] Y. Xi, K.-W. Sha, W.-Sg Shi, L. Schwiebert and T. Zhang, “Probabilistic adaptive anonymous authentication in vehicular networks,” Journal of Computer Science and Technology (JCST 2008), vol. 23, no. 6, pp. 916–928, November 2008.

[42] J.- P. Hubaux and S. Capkun and J. Luo, “The Security and Privacy of Smart Vehicles,” IEEE Security & Privacy, vol. 2, no. 3, 2004

[43] N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” in Proc. 2nd ACM workshop on Wireless security (WiSe 2003). ACM WiSe 2003, 2003.

[44] A. Vora and M. Nesterenko, “Secure location verification using radio,” in Proc. 8th International Conference Principles of Distributed Systems. OPODIS, 2004, pp.369–383.

[45] T. Leinm¨uller and E. Schoch and F. Kargl, “Position Verification Approaches for Vehicular AdHoc Networks,” IEEE Wireless Commun., vol. 13, no. 5, pp. 16–21, 2006.

[46] E. Schoch and F. Kargl and T. Leinm¨uller, “Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification,,” in Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET). ACM VANET ’06, 2006.

[47] J.-H. Song and V. W. S. Wong and V. C.M. Leung, “A framework of secure location service for position-based ad hoc routing,” in Proc. 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, 2004, pp. 99–106.

[48] Hassan Hadi Salih, “IMPLEMENTATION of ELECTRONIC SYSTEM PARTICULARLY to CANDIDATES APPLYING for ADMISSION to PEASS COLLEGES”, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 5, Issue. 6, June 2016, pp.61–70.

[49] J. Zhao and G. Cao, “VADD: vehicle-assisted data delivery in vehicular ad hoc networks,” IEEETrans. Veh. Technol. (TVT 2008), vol. 57, no. 3, pp. 1910–1922, 2008.

[50] A. Skordylis and N. Trigoni, “Delay-bounded routing in vehicular adhoc networks,” in Proc. 9th ACM international symposium on Mobile ad hoc networking and computing, 2008, pp. 341–350.

[51] B. Jarupan and E. Ekici, “PROMPT: A cross layer position-based communication protocol for delay-aware vehicular access networks,” Ad Hoc Neworks Journal Special Issue on Vehicular Networks, vol. 8, no. 5, pp. 489–505, July 2010.

[52] V. Namboodiri and L. Gao, “Prediction-based routing for vehicular ad hoc networks,” IEEE Trans. Veh. Technol., vol. 56, no. 4, 2007

[53] S. Biswas, R. Tatchikou, and F. Dion, “Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety,” IEEE Commun. Mag., vol. 44, no. 1, pp. 74–82, 2006.

[54] C.E. Palazzi and S. Ferretti and M. Roccetti and G. Pau and M. Gerla, “How Do You Quickly Choreograph Inter-Vehicular Communications? A Fast Vehicle-to-Vehicle Multi-Hop Broadcast Algorithm, Explained,” in Proc. 4th IEEE Consumer Communications and Networking Conference. IEEE CCNC 2007, 2007, pp. 960–964.

[55] Z. Niu, Q. N. W. Yao, and Y. Song, “Study on QoS Support in 802.11ebased Multi-hop Vehicular Wireless Ad Hoc Networks,” in Proceedings of 2007 IEEE International Conference on Networking, Sensing and Control. IEEE, 2007, pp. 705–710.

[56] W. Yao, Q. Ni, Y. Song, and Z. Niu, “DeReQ: a QoS routing algorithm for multimedia communications in vehicular ad hoc networks,” in Proc. International Conference on Wireless Communications and Mobile Computing (WCMC 2007). IEEE, 2007, pp. 393–398.

[57] T. Kwon, Y. Lee, H. Lee, N. Choi, and Y. Choi, “Macro-Level and Micro-Level Routing (MMR) for Urban Vehicular Ad Hoc Networks,” in Proc. IEEE Global Telecommunications Conference (GLOBECOM ’07). IEEE GLOBECOM ’07, 2007, pp. 715–719

[58] K. Bilstrup, E. Uhlemann, E. Stroom, and U. Bilstrup, “On the Ability of the 802.11 p MAC Method and STDMA to Support Real-Time Vehicle-to-Vehicle Communication,” Journal on Wireless Communications and Networking, vol. 2009, pp. 1–13, January 2009.

[59] C. Chigan, V. Oberoi, J. Li, “RPB-MACn: A relative position based collision-free mac nucleus for vehicular ad hoc networks,” in IEEE GLOBECOM 2006. IEEE GLOBECOM 2006, 2006.

[60] K. A Redmill and M.P. Fitz and S. Nakabayashi and T. Ohyama and F. ¨Ozg¨uner and U. ¨Ozg¨uner and O. Takeshita and K. Tokuda and W. Zhu, “An incident warning system with dual frequency communications capability,” in Proc. IEEE Intelligent Vehicles Symposium, 2003. IEEE, June 2003, pp. 552–557.

[61] M. Torrent-Moreno and P. Santi and H. Hartenstein, “Distributed Fair Transmit Power Assignment for Vehicular Ad Hoc Networks,” in Proc. the 3rd Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), vol. 2. IEEE SECON 2006, 2006, pp. 479–488.

[62] V. Kawadia and P.R. Kumar, “Principles and protocols for power control in wireless ad hoc networks,” IEEE J. Sel. Areas Commun., vol. 23, pp. 76–88, 2005.

[63] L. Yang, J. Guo, and Y. Wu, “Channel Adaptive One Hop Broadcasting for VANETs,” in Proc. 11th International IEEE Conference on Intelligent Transportation Systems, 2008.

[64] A. Kovacs, “Resource Sharing Principles for Vehicular Communications,” in Proc. IEEE GLOBECOM Autonet 2008 workshop, 2008, pp. 1–10.

[65] R. Ramanathan and R. Rosales-Hain, “Topology control of multihop wireless networks using transmit power adjustment,” in Proc. IEEE Nineteenth Annual Joint journal of the IEEE Computer and Communications Societies, INFOCOM’00, vol. 2. IEEE INFOCOM ’00, 2000, pp. 404–413.

[66] C. Chigan and J. Li, “A delay-bounded dynamic interactive power control algorithm for VANETs,” in IEEE International Conference on Communications, 2007. IEEE ICC ’07, 2007, pp. 5849–5855.

[67] X. Yang and L. Liu and N.H. Vaidya and F. Zhao, “A vehicle-tovehicle communication protocol for cooperative collis+ion warning,” in Proc. 1st Annual Intl. Conf. Mobile and Ubiquitous Syst: Networking and Services, 2004, pp. 114–123.

[68] Y. Zang, L. Stibor, X. Cheng, H.-J. Reumerman and A Paruzel and A. Barroso, “Congestion control in wireless networks for vehicular safety applications,” in Proc. 8th European Wireless Conference, 2007.

[69] M. Torrent-Moreno, D. Jiang and H. Hartenstein, “Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks,” in Proc. 1st ACM international workshop on Vehicular ad hoc networks. ACM New York, NY, USA, 2004, pp. 10–18.

[70] J. Peng and L. Cheng, “A distributed mac scheme for emergency message dissemination in vehicular ad hoc network,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3300–3308, 2007.

[71] A. Hassan, M. El-Shehaly, and A. Abdel-Hamid, “Routing and reliable transport layer protocols interactions in MANETs,” in Proc. International Conference on Computer Engineering & Systems (ICCES ’07. ICCES ’07, 2007, pp. 359–364.

[72] M. Bechler, S. Jaap, and L. Wolf, “An optimized tcp for internet access of vehicular ad hoc networks,” Lecture Notes in Computer Science, vol. 3462, pp. 869–880, 2005.

[73] R. Schmilz, A. Leiggener, A. Festag, L. Eggert, and W. Effelsberg, “Analysis of path characteristics and transport protocol design in vehicular ad hoc networks,” in Proc. IEEE 63rd Vehicular Technology.

[74] Muhammed Abaid Mahdi, Saad Talib Hasson , “A Contribution to the Role of the Wireless Sensors in the IoT Era”, Journal of Telecommunication, Electronic and Computer Engineering, University of Babylon, October 2017, e-ISSN: 2289-8131 Vol. 9 No. 2-11

[75] S. T. Hasson and Z. Y. Hasan, "Roads clustering approach's in VANET models," 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, 2017, pp.316-321. doi: 10.1109/NTICT.2017.7976140