IJCTA, 9(12), 2016, pp. 5805-5814

A Survey on Various Routing Protocols for Vanet

***J.S. Vimali **Mekala Harinath Reddy**

Abstract : In recent days, prospect of vehicular ad hoc network (VANET) is shifting into an fascinating investigation area; it could be a mobile ad hoc network believed-about as a peculiar event of mobile ad hoc network (MANET). Like manet, It is qualified as self- directed and self-set up wireless network. Nevertheless, it has atrociously active network topology, massive and adjusentry network scope, and filtered mobility; these features directed to obligation for reasonable direction- finding and resource convertible protocols, to ensemble through entirely diverse situations. These differences condense old-fashioned MANET's protocols inappropriate for VANET. Purpose of this effort is to convey a study of VANETs expelling contrivances, this paper suggestions a precipitate of transport ad hoc networks and therefore existing VANET expelling protocols; predominantly it directed on device to device (D2D) dissemination and protocols. This paper moreover signifies complete summaries and aims, examines completely unlike expelling systems that are established. Furthermore as if arrangements of expelling protocols (focusing on two taxonomies forms), and offers concise evaluations between entirely diverse groups within background of their procedures used, strong point, and limits of every category theme matched to diverse groups. Lastly, it abstracts these styles and therefore challenges for economical expelling mechanisms.

Keywords : VANET, Route, Routing Protocols, Topology-based, Location-based, D2D.

1. INTRODUCTION

Vehicular ad hoc networks are a distinct chic of mobile ad hoc networks; wherever devices square measure replicated as mobile nodes. it comprises 2 entities: access points and devices, access points are fastened and typically coupled to network, and that they may contribute as a dissemination drive for devices [1]. It discourses wireless dissemination between devices (D2D), and between devices and infrastructure (D2I). Device to device dissemination (D2D) has 2 methods of dissemination: one step dissemination, and multi-step dissemination. It conjointly has distinct features that discriminate it from unlike mobile ad hoc networks; foremost necessary features are: great quality, group, disseminated dissemination, road boundaries, and no constraint of network scope [2]-[4], of these features created setting a difficult for emerging economical expelling protocols. ITs presentations varieties square measure categorized into protection and potency presentation [1], [5], [6]. There are numerous hitches facing it systems style and employment, including: safekeeping, secrecy, directing, property, and quality of amenities. This paper can target expelling downside in device to device dissemination (D2D);

Main objective for expelling protocol is to produce optimum ways among network nodes via least overhead. Several expelling protocols are developed for its atmosphere, which might be classified in many ways, in step with completely different aspects; such as: protocols features, techniques used, expelling info, quality of services, network structures, expelling algorithms, and so on. Some analysis papers classified VANETs expelling protocols into 5 classes: topology-based, location-based, geocast-based, broadcast, and cluster-based expelling protocols, this taxanomies relies on expelling protocols features and techniques used [2], [5], [7]. As well, different papers classified its expelling protocols in step with network structures, into 3 classes: hierarchic expelling, flat expelling, and location-based expelling. Moreover, they'll be classified into 2 categories in step with expelling strategies:

* Asst. Professor, Department of Information Technology, vimalijsmtech@gmail.com,

** Department of Electronics and Communication Engineering, Sathyabama University, Chennai, India. 2harinath.m1995@gmail.com

proactive and reactive [8]. On different opposite hand other papers classified them into 2 categories: geographic-based and topology-based, in step with expelling info employed in packet forwarding [4]. Conjointly supported quality of services taxonomies, there are 3 forms of protocols that coping with configuration (hierarchical, flat, and location aware), regarding with route identification (reactive, proactive, hybrid and predictive), or supported raincoat layer interaction [9]. But all earlier taxonomies didn't concern by announcement ways taxonomies (such as unicast, broadcast, and multicast).

This paper can reference on expelling protocols supported expelling info that employed in packet forwarding, it in main focuses on topology-based and location-based routing.

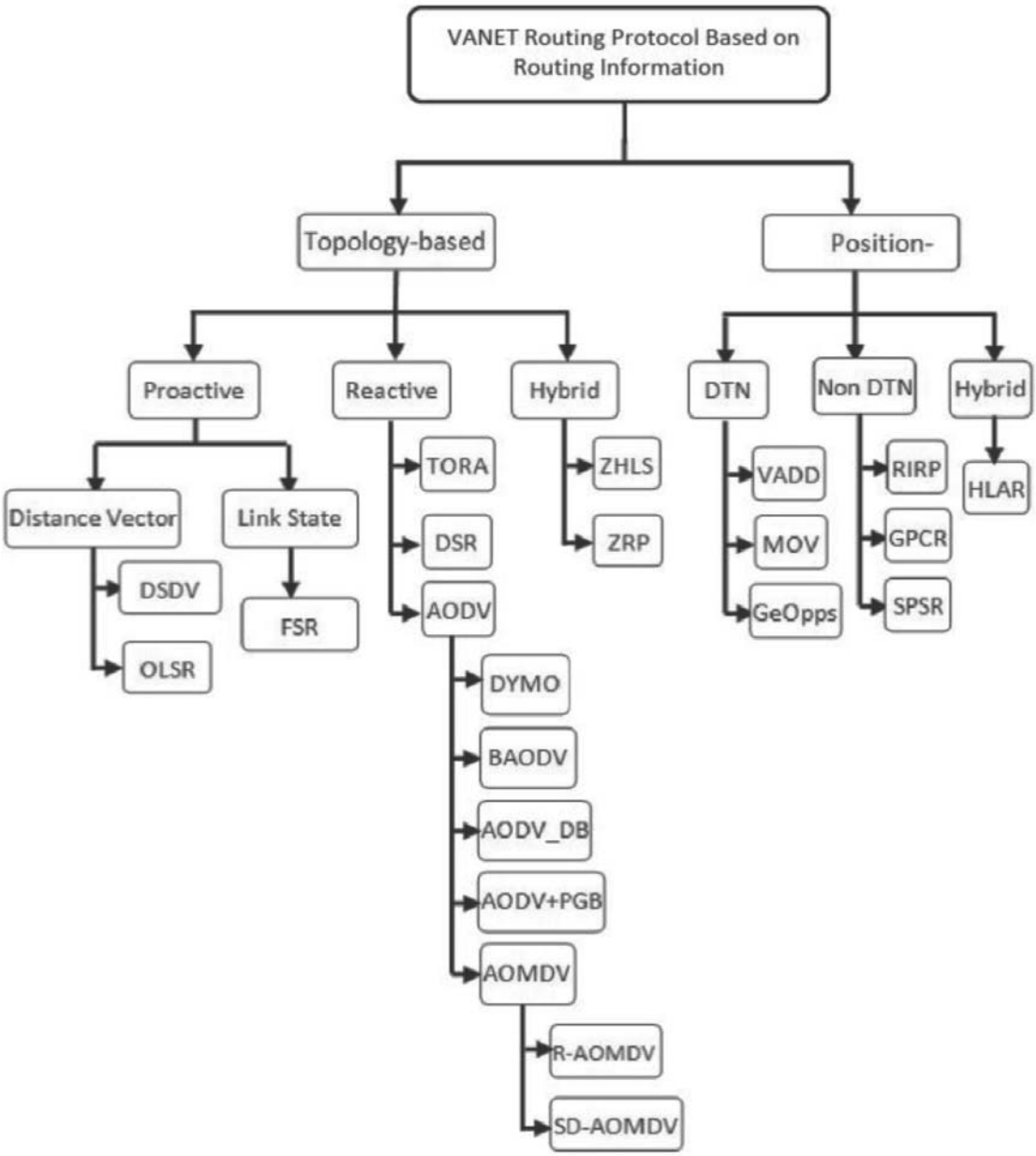

Fig. 1. Classification of VANET routing protocols.

2. ROUTING DATA UTILIZED IN PACKET FORWARDING

Such category is split hooked on 2 taxonomic category: topology-based and location-based expelling protocols. In topology-based expelling, every device ought to remember of network design, conjointly ought to able to frontward packets victimization data concerning offered nodes and links within network. In distinction, location-based expelling ought to remember of places within packet forwarding.

A. Topology-Based Routing Protocol

Topology-based expelling protocol typically a conventional, it practices connection's data that hold on within expelling bench as a basis to frontward packets from origin device to end; it usually classified into 3 classes[3],[10]: Proactive (periodic), Reactive (on-demand) and Hybrid

1. Proactive Routing Protocols

Proactive protocols permit a network device to use expelling entry to store routes data for all alternative nodes, every access within stand contains succeeding step device utilized in trail to terminus, no matter whether or not route is really required or not. Entry should be updated often to mirror topology changes, and may be broadcast periodically to neighbors. This theme might cause a lot of overhead particularly within high quality network. However, routes to terminus can invariably be offered once required [4]. Proactive protocols typically rely on undeviating path algorithms to work out that route are chosen; they typically use 2 expelling strategies: Link state strategy and distance vector strategy.

(*a*) Destination Sequence Distance Vector Routing (DSDV) : DSDV protocol it's associate initial circumstantial expelling protocol, it apparatuses space vector approach and uses a shortest path rule to implement just one route to terminus that hold on within expelling entry, every expelling entry contains data concerning all reachable network nodes, in addition because whole variety of trips required to succeed, every access within expelling entry is categorized with a structure variety originated terminus device. To take care of routes liableness, every device should periodically broadcast its expelling entry to its neighbors. However, DSDV will improve overhead within giant network; attribuentry to uncalled-for change broadcast although there's no change within topology. Besides that, DSDV do not offer multi routes to terminus device [8] and has no management over network bottleneck that decreases expelling potency [11].

(*b*) Optimized Link State Routing Protocol (OLSR) : OLSR protocol instrument relation state strategy; it keeps a expelling entry covers info concerning all potential routes to network nodes. Once topology is modified every device should send its rationalized info to some discriminating nodes that transmit this info to its alternative selective nodes. Nodes that don't seem to be within chosen list will simply browse and method packet [10]. Some researchers thought that OLSR has straightforward procedure that permits it to intrinsically completely different in operation systems, besides it works well within dynamic topology, conjointly it's usually appropriate for applications that needed low latency within knowledge transmission (like warning applications) [11]. However, OLSR could cause network congestion; due to frequent management packets that sent to handle topology changes, what is more OLSR ignore high resources capabilities of nodes (like transmission vary, bandwidth, antenna and then on) [12]. Therefore, some researchers propose hierarchical Optimized Link State Expelling (HOLSR) protocol as sweetening of OLSR protocol, that decreases expelling management overhead within massive size networks, conjointly maximizes expelling performance; by shaping network hierarchy design with multiple networks [13].

(*c*) Fuzzy State Routing (FSR) : In FSR, device occasionally bring up-to-date its entry supported newest info established from adjoining nodes. Change of expelling entry entries that anxiety a particular terminus should be transmission by completely diverse incidences for neighbors. However, it may well be correct, if packets return nearer to terminus [4], [14]. What is more if terminus travels out of choice of source device then it can't discover route [4], [15]. benefit of proactive expelling protocols may be abbreviated to there's no have to be compelled to route identification process; as a result of route to terminus is unbroken within background, what is more proactive protocols periodically update expelling info that lets these protocols to perform well in low quality networks. However, they need degraded performance in extremely quality and density network that once compare them with reactive expelling

protocols, what is more unused routes consume offered information measure and improve network overhead [2]. Recent studies show that proactive expelling protocols (such as OLSR) usually outgo reactive protocols in terms of network turnout and finish to finish delay [16]. However; there's no a lot of analysis within proactive expelling protocols for compared with existing reactive protocols researches**.**

2. Reactive Routing Protocols

Reactive expelling protocols (also known as on-demand) cut back network overhead; by maintaining routes only required, that origin device starts a route identification method, if it desires a non-existing route to a terminus, it will this method by flooding network by a route request message. When message reaches terminus device (or to device that encompasses a route to terminus), this device can send a route react message back to origin device exploitation unicast dissemination [17]. Reactive expelling protocols area unit applicable to massive size of mobile accidental networks that area unit extremely quality and frequent topology changes [18]. Several reactive expelling protocols are developed, subsequent sections can illustrate characteristic of some reactive protocols, also as illustrates present improvement protocols.

(*a*) Accidental on-Deman Distance Vector (AODV) : AODV expelling protocol is planned for mobile accidental network, it's been evaluated in many researches and shows sensible results compared to connected expelling protocols; thus it's a decent documentation [19]. AODV offers low network overhead by reducing messages flooding within network; that in comparison to proactive expelling protocols, besides reducing necessity of memory size; by minimizing expelling entrys that keep solely entries for recent active routes, additionally keeps next step for a route instead of entire route. It additionally provides dynamically updates for adapting route conditions and eliminates process in routes; by exploitation terminus sequence numbers. Thus AODV is versatile to extremely dynamic constellation and large-scale network [20]. However, it causes giant delays during a route identification, additionally route failure could need a brand new route identification that crops extra delays that decrease information transmission rate and improve network overhead [17]. Moreover, redundant broadcasts while not management can consume additional information measure (broadcast storm problem), this drawback grows because variety of network nodes will improve, that besides collisions that cause data lost drawback [19]. There are a unit many protocols are planned to boost AODV protocol; by decreasing its issues.

(*b*) Dynamic Source Routing Protocol (DSR) : DSR protocol aims to origin a extremely reactive expelling process; by implementing a expelling mechanism with a very low overhead and quick reaction to frequent network changes, to ensure thriving knowledge data delivery no matter network changes. DSR may be a multi- step protocol; it decreases network overhead by reducing periodic messages. This protocol has 2 main processes: route identification and route Maintenance. Within route identification, once a origin device wants an unobtainable route, it initially broadcasts a route quest message. All intermediate nodes that received this message can send it, except if it absolutely was terminus device or it's a route to terminus; during this case device can send a route replay message back to origin, later received route is paid within origin expelling entry for future use. If a route is failing, origin nodes are enlightened by a route error message. In DSR protocol, each knowledge data contains a whole list of intermediate nodes; therefore origin device ought to delete unsuccessful route from its cache, and if it stores different thriving route thereto terminus in its cache, it'll exchange unsuccessful one by opposite thriving route. However if there's no different route, it'll initiate a replacement route identification method. Advantage of DSR protocol is clearly shown in a very network with low mobility; as a result of it will use choice route before starts a replacement method for route identification. However, multi routes might cause extra expelling overheads by adding all route info to each knowledge data, besides, because network span larger distance and together with a lot of nodes, overhead can frequently improve and as result network performance are degraded.

(*c*) Temporally Ordered Routing Formula (TORA) : TORA may be a distributed expelling protocol victimization multi step routes; it's designed to cut back dissemination overhead associated with adapting frequent network changes. This protocol doesn't implement a shortest path algorithm; therefore expelling structure doesn't represent a distance. TORA constructs a directed graph that contains origin device because tree roots. Dataought to be running from higher nodes to lower nodes within tree. Once a device broadcasts a data to a selected terminus, its nearer can broadcast a route replay if it's a downward link to terminus, if not, it simply drops data, since data forever flows downward to terminus and do not flow upward back to causation device Benefits of TORA area unit that it offers a route to each device within network, and reduces management messages broadcast. However, it causes expelling overhead in maintaining routes to any or all network nodes, particularly in extremely dynamic [4], [15].

3. HYBRID ROUTING PROTOCOLS

Hybrid protocol may be a mixture of each proactive and reactive protocols; it aims {to minimize to attenuate to cut back} proactive expelling protocol management overhead and reduce delay of route identification method inside on- demand expelling protocols. Typically hybrid protocol divides network to several zonas to supply a lot of liableness for route identification and maintenance processes. [3].

(*a*) Zona Routing Protocols (ZRP) : ZRP is that 1st protocol developed as a hybrid expelling protocol, it permits a network device to divide network into zonas per several factors; like: power of transmission, signal strength, speed and plenty of different factors. space| world| realm} within zona is that expelling vary area for device and contrariwise for outdoor zona. ZRP uses reactive expelling schemes for outdoor zona and therefore proactive expelling schemes for within zona; with a read to stay most recent route info inside within zona. Within native within zona, origin device uses a proactive cached expelling entry to initiate a route to a terminus, which might be helped in sending data's directly immediately. ZRP uses freelance protocols within and outdoors zone; it's going to use any existing proactive and reactive expelling protocols. For outdoor zona, ZRP reactively discover a route; that origin device transmits a route quest data to border nodes of its expelling zona; data includes a singular sequence range, origin reference and therefore terminus reference. Once border device receives a route quest data, it's for terminus inside it's within zona. If terminus is found, it sends a route react on reverse path to origin device; else if it does not realize terminus in its native zona, border device adds its reference to route quest data and forwards it to its own border nodes. Once origin received a react, it stores trail enclosed within route react data to use it for knowledge transmission to terminus. Weakness of ZRP protocol is that it performs sort of a pure proactive protocol significantly for giant size zonas; but for tiny zonas it performs like a reactive protocol [17]. Therefore ZRP protocol isn't applicable for giant size with extremely dynamic topology and regularly change environment.

(*b*) Location-Based Routing Protocol : Location or geographic expelling protocol relies on point info in expelling process; wherever origin sends a data to terminus victimization its geographic location instead of victimization network reference. This protocol needed every device is ready to decide its location and therefore location of its neighbors through Geographic Location System (GPS) help. Device identifies it's nearer as a device that set within device's radio vary. once origin got to send a data, it always stores location of terminus within data header which is able to facilitate in forwarding data to terminus while not must route identification, route maintenance, or may be awareness of configuration [3], [4]. Therefore location expelling protocols area unit thought-about to be a lot of sentry and appropriate with a high quality atmosphere, compared to topology-based expelling protocols. Geographic expelling protocols normally classified into 3 classes: Delay Tolerant Network (DTN) Protocols, Non Delay Tolerant Network (Non DTN) Protocols and hybrid [4].

4. Delay Tolerant Network (DTN) Protocols

DTN may be a wireless network designed to perform expeditiously in networks with some features; like frequent disconnection dissemination, giant scale, long inescapable delays, restricted information measure, power constraints and high bit fault rates [15]. During this network, all nodes facilitate one another to forward datas (store and forward scheme). These nodes might have a restricted transmission range; therefore datas transmission can take giant delays. Commonly, DTN device may be a mobile device, therefore it establishes routes to different nodes after they reach its transmission vary. In DTN protocol, there's no guarantee of unbroken finish to finish property, that datas is also cached for a time at intermediate nodes [4], [14], [3]. To style of an expelling protocol for DTN network with these features may be a vital downside. This section, review several DTN expelling protocols that constitute this class.

(*a*) Motion Vector Routing algorithm (MOVE) : MOVE algorithmic program is meant for lightweight networks, particularly for road aspect device dissemination. This protocol assumes that every device has world locations info, which is beside data of a mobile router speed and its neighboring nodes rate. From this info device will estimate nodes that area unit nearest distance to terminus [14]. During this protocol every device frequently broadcasts a howdy message; and it's nearer replays by a RESPONSE message; by this replayed message device can understand its neighbors and their locations. Given this info, device will estimate shortest distance to terminus, in this case device decides a way to forward message in step with data concerning nodes that area unit presently set near terminus. MOVE protocol uses less memory size compared with Non DTN location-based expelling; it conjointly features a higher knowledge transmission rate in lightweight environments [30]. However, Non DTN location-based expelling may have higher performance given that routes area unit sentry and consistent [3].

(*b*) VADD: DEVICE-ASSISTED knowledge DELIVERY IN conveyance impromptu NETWORKS : VADD protocol designed to handle often disconnected conveyance networks and extremely quality issues. It implements shop and forward scheme; whereas a device is moving it stores data, till a replacement device arrives to its zona vary, then it forwards keep data to current new device. This protocol predicts device quality supported 2 factors:

Network traffic and route type, which facilitates a device to find successive forwarding device. VADD protocols typically deliver data to trail with smallest amount transmission delay; following 3 main principles [4], [14].

- Continue use accessible wireless channel
- Deliver data to upper speed device within route to hold it
- It may be a high quality atmosphere, therefore it's tough to estimate data delivery by a predefined optimum path, which can result in frequent discover a replacement optimum path to transmit a data. To interrupt expelling loop, every device adds info concerning its former step/hops before forwarding data, containing its own info as a former step. Once data received to a device, it's at previous hops info to avoid forwards data to previous hops and take a look at to seek out different accessible step; so might avoid expelling loop downside. To forward a data, VADD implements four totally different schemes [4], [14]:
- Location first Probe (L-VADD):
- Direction first Probe (D-VADD):
- Multi-Path Direction initial is that Probe VADD (MD- VADD):
- Hybrid Probe VADD (H-VADD

(*c*) Geographical Opportunistic Routing (GEOPPS) : GeOpps may be a forwarding protocol uses accessible navigation system in assembling info concerning geographical location; this info is employed to pick devices that area unit nearest to a particular terminus. Protocol uses store and forward technique; it

works rather like Move and Non DTN protocols however it uses navigation system to supply economic data delivery. Within GeoOpps, to send a data from origin to terminus, there are a unit 3 main steps accustomed choose successive step of intermediate nodes [3], [5]:

- Every neighboring device at calculable routes calculates longer term nearest purpose to terminus that it will reach presently.
- Every nearer device then calculates calculable shortest delay time to achieve required data's terminus.
- Use calculable shortest time calculated by every nearer device; that any device calculable to be nearer to terminus in lowest delay time, ought to be chosen to become successive step carrier to transmit data quicker to required terminious. Protocol involved some cases that have an effect on its potency [3], [5]:
- Device ignores calculable calculated route and follows different totally different path; during this case system can
- Device stops its movement (switch off engine or long pause time); during this case its datas ought to be forward to a different neighboring device. Good thing about GeOpps doesn't need all nodes to calculate routes; and GeOpps transmission rate depends solely on route topology and therefore quality of nodes. However, it's some complexities in scheming delay time looking on a navigation system measure.

5. Non Delay Tolenant Network (NON DTN) Protocols

Non-DTN protocols area unit geographic expelling protocols, however it doesn't think about a dis-connectivity issue; it assumes there are a unit invariably variety of nodes to realize sure-fire dissemination; therefore, this protocol is simply appropriate for prime density network. In these protocols, device forwards its data to nearest nearer to terminus; however this approach is also unsuccessful if there's no nearest nearer to terminus instead of this device itself. Several non-DTN expelling protocols handle this failure; by totally different ways are going to be shown within following sections [1].

(*a*) Greedy Perimeter Source Routing (GPSR) : GPSR may be a celebrated greedy expelling protocol. During this protocol, every device forwards datas to different intermediate nodes that area unit perpetually nearer to data's terminus (greedy forward), till data reaches its final terminus. If there's no neighboring device near terminus, it uses perimeter forwarding to make your mind up to that device it'll deliver data. GPSR may be a homeless protocol that keeps info of its initial step nearer's positions that may improve protocol quantifiability quite shortest path impromptu expelling protocols. Another advantage is that dynamic forwarding datas call [3]. However, GPSR may face a link failure owing to high quality network and frequent topology changes (it holds previous location information). This downside are often handled by perimeter forwarding, however it should cause high data loss and a lot of latency time owing to big range of hops in perimeter forwarding mode. Moreover, if terminious device moves to a replacement location, its info that embedded within data header can ne'er be updated [2].

(*b*) Greedy Perimeter Stateless Routing (GPCR) : GPCR protocol is meant to be appropriate for high quality environments (as in city) supported greedy forwarding technique; this system aims to forward data to a nearer device that is nearest to situation of terminus. Every device has got to bear in mind of its location gotten by a navigation system, it is aware of its nearer by periodic beaconing, and therefore location of terminus is obtained from situation service. Once a device forwards a data, datas are going to be meet road till it reaches successive intersection. Up keep method covers 2 components: higher cognitive process, to make your mind up that intermediate device data are going to be passed on intersection (an organizer device selection), and forwarding data to successive intersection. Organizer device decides to that route datas are going to be forwarded. However if no organizer device found within route, data are going to be forwarded to furthest device [10]. GPCR doesn't would like any world information; but it's supported property of terminus device and therefore density of successive roads, it couldn't connect terminus if device density is low, which is able to improve transmission delay [18].

(*c*) Reliability-Improving Location-Based Routing (RIRP) : RIPR may be a location-based expelling algorithmic program designed, it aims to resolve issues of links failures that found in an exceedingly location-based expelling; that seem owing to storing previous info a few stale intermediate nodes. RIPR predicts device speeds and their moving directions, in addition as estimates features of town road. during this protocol, sender selects Associate in Expelling intermediate device to forward its data, supported quality estimation for neighboring nodes that done by ab initio deciding whether or not a nearer device exists or not. sender creates a foothold store for every neighboring device, this store contains recent location of device and its quality speed; that helps within choice of forwarder device that is completed supported route features and therefore device location store that organized when exchange of beacon messages. This store avoids native downside that prevents a device to pick a nearer device as a forwarder device; that happens as a result of there's no device that's nearest to terminus. RIPR protocol is analogous to GPSR protocol uses 2 modes: a greedy mode and perimeter mode, in addition because route features thought, and therefore location of nodes. Therefore, RIPR will therefore link failure downside caused by storing info a few stale intermediate device; so it will reduce chance of link failure [18].

6. Hybrid Location-Based Routing

Location expelling protocol reduces management expelling overhead, it does not got to construct or maintain a expelling entry; as a result of it solely uses situation info concerning neighbors and terminus nodes, these problems created location-based Expelling protocols ascendable.

However, location expelling protocols have several limitations that prohibit their usage; these limitations are often summarized within following points [6]:

- Performance of location expelling are often considerably minimized in step with situation accuracy; as a result of correct locations info is a vital issue to urge an honest performance in location expelling.
- Location expelling may be failing, if there's no any nearer device that is nearer to terminus (null area).
- Location expelling solves absence of nearest nearer toward terminus, by backup method. However, it needed datas to travel larger distances to achieve terminus, conjointly datas may be travel in an exceedingly shut circle, or may be born. Therefore no existing expelling protocol performs expeditiously all told circumstances. Therefore, several researchers developed hybrid schemes, they merge features of 2 or a lot of location-based expelling protocols (non-DTN and DTN schemes), generally they merge one or a lot of topology expelling protocols (reactive, proactive and hybrid schemes) with location-based expelling. Hybrid location expelling protocol may be a mixture protocol that takes advantage of quite one protocol schemes. Successive section can illustrate HLAR protocol that being Associate in Expelling example of may be a hybrid location-based expelling protocol.

(*a*) Hybrid Location-Based impromptu Routing Protocol (HLAR) : HLAR may be a hybrid location expelling protocol designed to expeditiously use all accessible location info and to attenuate expelling management overhead. This protocol is planned to change to on-demand expelling once adequate location info is unprocurable or restricted, it conjointly deals with matter of no nearest nearer to terminus (void regions), and then it's nearly a ascendable protocol. HLAR works as a reactive protocol within route identification method, but if there's no route to terminus device, origin device adds info concerning its location and therefore location of terminus within route quest data then it searches for a more in-depth device close to terminus. If device finds a nearer that is near terminus then it forwards quest data thereto. Origin device repeats these steps till it reaches required terminus. Simulation results showed that HLAR protocol minimizes expelling management overhead compared with on-demand expelling protocols, what is more it usually provides contemporary giant size location info [6]. However, HLAR does not guarantee simplest reliable route; as a result of intermediate device does not have a reverse link to origin, and will not inform different neighboring nodes if it finds a much better route to origin [19].

However, it's tougher to seek out a particular expelling protocol that works expeditiously all told network atmosphere situations; that some protocol is also appropriate for high quality atmosphere however suffer from finish to finish delay, in distinction different protocols may offer quick data delivery, however unsuientry for high quality atmosphere, and so on. therefore it may be tough work to exactly compare present expelling protocols, or maybe claims that one is that best all told atmosphere situations; but some analysis papers analyzed 2 categories and compare them victimization some connected protocols; and their results is finished that location-based expelling performs higher than topology-based expelling for each urban and rural situations [20].

3. CONCLUSION

This paper has presented an summary of vehicular s ad hoc networks, illustrates their motivation and features, it studied in detail VANETs expelling downside, principally device to device (D2D) dissemination, providing two taxanomiess of VANETs expelling protocols that exist within previous couple of years, investigated them and showing however do they work and their main advantages and limitations

4. REFERENCES

1. Ramin Karimi, Norafida Ithnin, Shukor Abd Razak, and Sara Najafzadeh, "Non DTN Geographic Routing Protocols forVehicular Ad Hoc Networks," *International Journal of Computer Science Issues (IJCSI)*, vol. 8, Issue 5, no. 3, September 2011.
2. Bijan Paul, Mohammed J. Islam, "Survey over VANET Routing Protocols for Device to Device Dissemination," *IOSR Journal of Computer Engineering (IOSRJCE)*, ISSN: 2278-0661, ISBN: 2278-8727, vol. 7, Issue 5 (Nov-Dec. 2012), pp. 01-09.
3. Moath Muayad Al-Doori, "Directional Routing Techniques in VANET," *PhD Thesis, Software Technology Research Laboratory, De Montfort University, Leicester United Kingdom*, November 2011.
4. Lee, Kevin C., Uichin Lee, and Mario Gerla., "Survey of Routing Protocols in Vehicular Ad Hoc Networks," *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges reference, IGI Global*, 2010, pp. 149-170, 25 Mar. 2013.
5. Salim Allal and Saadi Boudjit, "Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal," *Journal of Internet Services and Information Security (JISIS)*, vol. 3, no. 1/2, pp. 20-36, February 2013.
6. Mohammad Al-Rabayah and Robert Malaney, "A New Hybrid Location-based Ad Hoc Routing Protocol," *Global Teledisseminations Conference (GLOBECOM 2010) IEEE* , vol. 1, no. 6, pp. 6-10, Dec. 2010.
7. Rakesh Kumar and Mayank Dave, "A Comparative Study of Various Routing Protocols in VANET," *International Journal of Computer Science Issues (IJCSI)*, vol. 8, Issue 4, no. 1, July 2011.
8. Vijayalaskhmi M., Avinash Patel, Linganagouda Kulkarni, "QoS Parameter Analysis on AODV and DSDV Protocols in a Wireless Network," *International Journal of Dissemination Network & Security*, vol. 1, no. 1, 2011.
9. lajos hanzo and rahim tafazolli, "Asurvey of QoS Routing Solutions for Mobile Ad hoc Networks," *IEEE Disseminations Surveys & Tutorials, 2nd quarte,* 2007.
10. James Bernsen and D. Manivannan,"Greedy Routing Protocols for Vehicular Ad Hoc Networks," *Wireless Disseminations and Mobile Computing Conference* IWCMC 08, vol. 632, no. 637, pp. 6-8, Aug. 2008.
11. Jamal Toutouh, Enrique Alba, "Optimizing OLSR in VANETS with Differential Evolution: A Comprehensive Study," *ACM DIVANet'11, Miami, Florida, USA.* 2011.
12. Sonam Jain and Sandeep Sahu, "Topology vs. Location based Routing Protocols in Mobile Ad hoc Networks: A Survey," *International Journal of Engineering Research & Technology (IJERT)*, vol. 1, Issue 3, May 2012.
13. Y. Lacharite and M. Wang, "Hierarchical OLSR draft-lacharite-manet-holsr-02," *Mobile Ad hoc Networking (MANET), IETF Internet-Draft,* 2009. [Online] Available: http://tools.ietf.org/html/draft-lacharite-manet-holsr-02 (July 13, 2009)
14. Yatendra Mohan Sharma and Saurabh Mukherjee, "A Contemporary Proportional Exploration of Numerous Routing Protocol in VANET", *International Journal of Computer Applications*, vol. 50, no. 21, pp. 14-21, July 2012.
15. Sandhaya Kohli, Bandanjot Kaur and Sabina Bindra, "A comparative study of Routing Protocols in VANET", *International Journal of Computer Science, Issues-IJCSI, Proceedings of ISCET*, 2010.

16. Johnson, David B., David A. Maltz, and Josh Broch. "DSR: dynamic source routing protocol for multi- step wireless adHoc networks," *Ad hoc networking 5*, pp. 139-172, 2001.

17. Chao Song, Ming Liu, Yonggang Wen, Jiannong Cao and Guihai Chen "Buffer and Switch: An Efficient Road-to-road Routing Scheme for VANETs", *Seventh International Conference on Mobile Ad-hoc and Sensor Networks*, 2011.

18. Si Ho Cha1, Min-Woo Ryu and Kuk-Hyun Cho, "A Survey of Greedy Routing Protocols for Vehicular Ad Hoc Networks," *Smart Computing Review*, vol. 2, no. 2, April 2012.

19. James. Jong Hyuk Park, Victor C.M. Leung, Cho- Li. Wang and Taeshik Shon, "Future Information technology, Applications, and Services", *FutureTech Springer,* vol. 1, pp. 82-98, 2012. [Online] Available:

    http://books.google.com/books?id=pggz UBASE4IC&prints ec=copyright#v=onepage&q&f=false (2012)

20. Akhtar Husain, Ram Shringar Raw, Brajesh Kumar and Amit Doegar, "Performance Comparison of Topology and Location Based Routing Protocols in Vehicular Network Environments", *International Journal of Wireless & Mobile Networks(IJWMN)*, vol. 3, no. 4, August 2011. [21] Gowri,S., Sathiyavathi, R. and Vimali,J.S. (2015)," Time-sensitivity based traffi control system ",Contemporary Engineering Sciences, Hikari, Vol. 8 , No. 1 , pp. 7-11, ISSN: 1313-6569.