***METHODOLOGIES TO IDENTIFY NON LINE OF SIGHT***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kaviarasan[1]Assistant Professor Dept of CSEAlpha college of Engg& TechPuducherry,Indiakaviarasanr64@pec.edu | Afraa Fathima[2]Dept of CSEAlpha college of Engg& TechPuducherry,Indiajulaikaz@gmail.com | Archanaa[3]Dept of CSEAlpha college of Engg& TechPuducherry,IndiaArchanaadhashi98@gmail.com | Chandralayka[4]Dept of CSEAlpha college of Engg& TechPuducherry,Indiachandraviji4@gmail.com | Suganthi[5]Dept of CSEAlpha college of Engg& TechPuducherry,IndiaSuganthisukku244@gmail.com |

**ABSTRACT**

An quality network to create risk free landscape which facilitate least clutterted up any risk free interaction betwixt vehicular nodes is vehicle ad hoc network (VANET). The challenges in VANET is transmission of security message betwixt vehicles during high cluttered environment. One of the major challenges in VANET is Non Line Of Sight (NLOS), in which broadcasting the data to crisis vehicle is being arduous. The vehicular nodes under NLOS situation should be figured effectively, so that the emergency vehicle can communicate to the NLOS node at accurate time period with decreased overhead were the time period depend upon the high degree of channel utilization. In this paper we are going to discuss many such methods proposed by researches by considering the advantages and drawbacks.

***Keywords:*** *VANET; NLOS; Broadcast; Road side unit; On board unit.*

# **Introduction**

Vehicular Ad hoc network based on ambulant junction (transport embedded with sensors), fixed foundation (Road Side unit) as well as wireless link towards allow them into provide aid on each further. The most important service provided by these networks is driving safety[1]. Almost 1.3 million people were passing on road calamity and extra 20-50 millions are get injured worldwide. Road calamity ranked as 9th leading cause of death[2]. Some survey shows that 60% of accidents can be avoided if the driver gets the warning even before half a second of the accident[3]. The World Health Organization published an International status report on road safety in December 2018, which reveals that the rate of road accident deaths has increased to 1.35 million each year[4]. It is reported that the foremost cause of death of people aged 5-29 years is road accidents. As per the National Crime Records Bureau report in 2016, 1.51 lakh people died in road accidents out of which 80.3 per cent of these accidents were a result of driver’s negligence[5]. The Federal Highway Administration states that around 2.5 million accidents occur in the junction each year[6]. Intersections are the second largest category of accidents about half of the severe crashes happen in junctures. Whereas easy as well as effective transmission VANET use two prominent technologies; IEEE 802.16 (Wireless MAN/WIMAX): Wireless transmission degree for MAN, designed into qualify multimedia application over wireless connections ranging up to 30 miles.

IEEE 802.11p (WAVE): Specially used for wireless way in transport domain. It enable V2V together with V2I transmission in the licensed ITS band of 5.9 GHz.

Types of communication [7] are

**Inter vehicular communication:**

This is also known as pure Ad-Hoc network which allows direct vehicular communication without need of any fixed infrastructure support.

**Road side communication:**

This type of network use a cellular gate way and wireless local area network access point to allow a vehicle to communicate with the roadside units mainly for information and data gathering application.

# **vanet issues**

Various issues in VANET [8] are

## 2.1Dynamic topology accompained by frequent disconnections

when vehicles are moving within that network they creates an very dynamic topology because when vehicle establishes an network interconnection using other vehicles into transfer an data packet or information. But while rate of the ambulant vehicles are changing as well as it is tough to maintain the same established connection as sometime the immediate neighbor node goes away of the wireless transference range. In this situation, source junction needs into look for some other junction into continue the meshwork connection. Where, the source node does not find the neighbor junction to continue the network connection because of junction density is low within the network or out of transference range. In real time this could be a critical problem and we support such case by pre-deploying of several relay junction or access points throughout the roads into maintain the meshwork connectivity.

## 2.2Computing Capacity with energy and storage

Every node is VANET is nothing but vehicle which should be equipped along ample amount of managing capabilities to process the raw data coming from other neighbor vehicles. Also, it needs proper storage capacity/energy to store/receive and transmit data for wireless transference. Electric power generation is not a critical issue for running VANET equipment in vehicles as they have rechargeable batteries which continuously generates power.

2.3Geographical position and transmission

Transport can be delivered with Global Positioning System (GPS) receivers which can help in delivering the locality information for routing occasion and ability to support transference in geographical areas to forward packets

2.4Numerous different transmissions environments

Usually, the transport operated in cities possess different building blocks & constructs and highways. Where fast, slow or stopped traffic is present. So there can be different types of road blocks encountered in each scenario for wireless data transmission in VANET.

2.5Delay restrictions and Real-time Transmission

Some of VANET applications which senses the collision, Pre-Crash or unexpected brakes, they need to generate the alerts for drivers or other automated vehicles. In such cases the maximum delay is crucial as a delay for more than the expected time results in collision/accidents. If information is received on time, accidents can be avoided.

2.6On-board sensors

Any vehicular ad hoc network node should be deliver with sensors having different potentiality which can be utilized for routing decision and forming transmission links.

2.7Infrastructure access

On account of ambulant nature of transport in VANET, the seamless conveyance & relativity is hard to be maintained. So conveyance infrastructures along the road side such as Roadside units (RSUs), access points, public hotspots etc.., will play an important role in cases where VANET hard delay constraints application are running in transports and for supporting continuous network connectivity & transmission.

2.8Variable network density:

Vehicular environment has varying thickness of vehicles depends upon congestion loads in various scenarios like congestion or less congestion in nights or it depends on locations etc

# **Non line of sight**

The vehicle to vehicle data exchange will be held with their radio communication range. But, in real life implementation, direct communication can be restricted and blocked by obstacles on the road preventing two vehicle from direct communicating with each other and creating a state of Non Line of Sight (NLOS) between them. Thus, preventing them exchanging proper data which will have an effect on localization service integrity and reliability[9]. Moreover, securing localization information under NLOS condition is yet a challenge.

3.1 Causes of NLOS

In VANET, many objects such as buildings, trees, and other constructions that exists on road sides can interfere or block radio signals .Moreover, moving objects on the roads can also cause signal block[10]. As vehicles come in different shapes and sizes, they can become an obstacle between neighbors that are in the same region of communications. Unlike buildings and fixed structure where interference and signal quality factors can be measured on field and be taken in consideration. Vehicles shapes (e.g, Trucks and Buses), mobility, formation and density can create obstacles that prevent direct communication between two nodes.

1. **NLOS SCENARIOS**

The different NLOS scenarios [11] are

## 4.1 Number of warning vehicle

In traffic safety applications, vehicles may send safety messages to other vehicles in order to prevent collisions or to ask for emergency services. We consider that vehicles may operate in warning, or in normal mode. Warning mode vehicles inform other vehicles about their abnormal status by sending warning messages periodically. Normal mode vehicles participate in the diffusion of these warning packets and, periodically, they also send beacons with information about themselves, such as their positions and speed. This factor is important since the more vehicles in the warning mode are there in a scenario, the more network traffic there will be, thus increasing redundant rebroadcasts which provoke heavy contention and long-lasting collisions. Figure 1 shows an example of a WMD scheme in a VANET.

## 4.2 The density of vehicle

In VANETs, the density of nodes can be particularly high, so when the number of node increases collision may occur which leads to NLOS situation.

## 4.3 The channel bandwidth

In radio communications, bandwidth is the width of the frequency band used to transmit the data. Channel spacing is a term used in radio frequency planning that describes the frequency difference between adjacent allocations in a frequency plan. The 802.11p [12] standard supports 10 and 20 MHz bandwidths. Using a 10 MHz bandwidth, the supported data rates are 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps, depending on the modulation and coding scheme considered. Since vehicular information delivery systems support applications such as cooperative driving among cars on the road, traffic safety, or infotainment applications, we think that channel bandwidth requirements could change based on the selected application. For the specific case of WMD mechanisms, the overall capacity of the channel can affect the effectiveness of warning dissemination schemes if the density of potential transmitters is high.

## 4.4 The broadcast scheme

Another important factor in Warning Message Dissemination in VANETs is the selected broadcast scheme. In VANETs, intermediate vehicles act as relays to support end-to-end vehicular communications. For applications such as route planning, traffic congestion control, and traffic safety, flooding of broadcast messages commonly occurs. However, flooding results in many redundant rebroadcasts, heavy channel contention, and long-lasting message collisions.



#### **Figure4.1:**Moving obstacle



#### **Figure4.2:**Fixed obstacle



#### **Figure4.3:**Intersection



#### **Figure4.4:**Hair pin curve



#### **Figure4.5:**Merging lane

1. **SURVEY**

Physical Obstacle and density of network can create obstacles that prevent direct communication between two nodes. Each vehicle maintains a database of its neighbor data that are updated by received beacons or by Bauer et al future an gain approach shadow map[13] for non-line of sight detection in city GNSS transport localization with VANET. Vehicle localization using satellite navigation systems like GPS is a suitable as well as achievable solution. Accurate location is a crucial requirement for many nowadays intelligent transport system its uses in the domain of consolation and security. As low-cost single-frequency GPS receivers are assumed to be standard in commercial vehicles global navigation satellite systems GNSS seem to be the most promising technology at the moment. Besides the accuracy of a steering solution the reliability and availability in terms of integrity are two major aspects of advanced localization systems as well. While satellite-based positioning reaches rather descent performance—e.g. street level-under good geometric constellation and open sky reception conditions—there are often situations with degraded exactness too. Especially when the focus of such applications is put into dense urban environments. in order to solve this problem in dense urban areas erroneous measurements caused by non-line-of-sight situations need to be handled carefully. the purpose of this paper is to evaluate shadow maps an efficient representation of satellite reception conditions for good real-time vehicle localization in urban areas. Instead of classical digital 3d maps which need to be installed and kept up-to-date at vehicle level shadow maps can be exchanged on demand with vehicular ad hoc networks. This approach developed within the European research project gain—is proven to increase exactness and probity of single-frequency receivers in urban areas without extra physical sensors. in addition to the positioning performance the necessary requirements for the transmission channel had been derived.

Sorrentino et all proposed an effective indicator for NLOS, and LOS channel dissemination condition[14]. A simple and physically-based index is proposed to identify among Line-of-Sight (LOS), near Line-of-Sight (NLOS) and Non-Line-of-Sight (NLOS) channel broadcast conditions. The index is based on the Generalized K (GK) fading model which has been proven to embody different channel dissemination conditions. Line-of-Sight (LOS) connection is highly desirable for user terminals.LOS or non-LOS (NLOS) transmission characteristics differ from each other. The radio channel model will be different in both LOS and NLOS conditions .A third channel condition defined near-LOS (NLOS) has been emphasized as the region in which an obstacles fall down in the First Fresnel zone to shadow the direct link between transmitting and receiving antennas. The first Fresnel zone can partially or totally obstruct the LOS region providing the NLOS and NLOS broadcast conditions. To detect and identify the wireless channel dissemination condition in terms of obstructions, several techniques have been proposed. An automatic procedure for characterizing the different wireless channel state by means of a physically-based synthetic indicator. The proposed indicator calls for an automatic procedure for the identification of the wireless dissemination channels. A simple, very effective and computationally efficient technique is proposed which, based on a proper combination of GK parameters is able to automatically discriminate among LOS, NLOS and NLOS channel state. This technique proposes a indicator, given by a actual mixture of parameters of GK fading model, which is operational effective since it is able to automatically regconize the typology of the channel condition. One of the major drawback in this paper is barrier within the first fresnel zone can partially or totally obstruct the LOS region providing the NLOS as well as NLOS broadcast condition.

SrdjanCapkun et al proposed the Authentication through Presence in Wireless Networks using integrity regions[15]. The main obstacle of widely deploying secure transmission between wireless nodes remains the cumbersome key setup process. We address this issue and introduce an IR (Integrity Regions) that enables message verification in wireless networks without use of reestablished keys.IR can be efficiently implemented with ultrasonic ranging but it is not used in distance enlargement. Two wireless devices trying to verify a shared secret key (e.g., using the Daffier-Hellman (DH) protocol could be subject to the known man-in-the-middle (MITM) attacks on the non authenticated DH protocol and therefore might not be able to established key securely. To overcome this shortcomings a security can be increased. Integrity regions (I Regions), a new security primitive that prevents MITM attacks on wireless communication through verification of presence. I Regions reply on range measurements to prevent distant attackers from inserting forged messages into the communication between the devices. In our approach, for each received message, the devices verify if it came from an expected distance (i.e., from their integrity regions). If the message came from the expected (safe) distance, it is accepted as authentic. The problem of key establishment can also be raised. It can be overcome by resurrecting duckling security policy model and in which key establishment is based on the physical contact between communicating parties. We know construct a Message Transfer authentication based on Integrity Regions (MT-IR). With this protocol, a device can verify the probity and the authenticity of messages received from other devices within its integrity regions. The major drawback in this paper if two wireless devices trying to initiate a shared secret key DH protocol could be subject to the man in the middle attack (MITM) on the noncertified DH protocol and therefore might not be able to begin the key securely.

Vanghefi et al proposed the Cooperative localization [16] because the accuracy of localization is highly degraded in indoor and harsh environments where source nodes either do not have connections with a sufficient number of anchor nodes due to strong attenuation or have very poor range estimates due to NLOS propagation. The Cooperative localization is a technique in which the source nodes communicate not only with the anchor nodes, but also with each other. Hence, the source nodes can collect several additional measurements which significantly improve the localization performance. Although many studies have examined NLOS-degraded localization of a static node in non-cooperative networks, and many others have examined the impact of cooperation for static localization, there is no work which considers cooperative tracking of mobile nodes. To address this open problem, in this work examine cooperative tracking, particularly in NLOS environments. More specifically, develop a novel sensor tracking algorithm based on Semi Definite Programming (SDP) which has the ability to mitigate NLOS propagation. This simulations show that the new SDP-based tracking algorithm outperforms the classic extended Kalman filter as well as the other recently proposed algorithms for non cooperative tracking in NLOS environments. Show that the algorithm can be extended to cooperative networks, and that a substantial performance benefit is realized by cooperation. It was found that tracking of NLOS biases is not beneficial as modelling NLOS propagation can be very difficult. Moreover the NLOS biases changes rapidly over the time which makes them difficult to track.

Osama Abumansor et all proposed an A cooperative multi hop location verification for NLOS[17] in VANET.In VANET, many objects such as buildings, trees, and other constructions that exists on road sides can interfere or block radio signals .Moreover, moving objects on the roads can also cause signal block [18]. As vehicles come in dissimilar shapes and sizes, they can become an obstacle between neighbors that are in the same region of communications. Unlike buildings and fixed structure where interference and signal quality factors can be measured on field and be taken in consideration .Vehicles shapes (e.g, Trucks and Buses), mobility cluster group messages. The neighbor data are monitored to detect any position and mobility inconsistency or expired record which will trigger the verification process. Node V is triggered to verify a neighbor C from its list. If V can’t verify C using direct communication or the interference is causing calculation error, it will transmit a verification request (Req) to its direct neighbors. The Req message contains (Reqid, Gid, IDc, Locc, Mc, IDv, Locv, Mv). If a node (Ni) receives the request it will verify the sender then checks if it has a direct communication with C or not. If it also don’t have a direct communication with C, it will mark C in its table as a node to be verified and forwards the message towards C. Before forwarding the message, node (Ni) listen to its neighbors and checks if any of them have forwarded the same message or not. If it was, it will ignore the forwarding process and waits for a reply. If it wasn’t forwarded and maximum number of hops wasn’t reached it will proceed to forward the message. The forwarded message contains the original request and adds (piggyback) its information as a sender and update the hop count. If a reply is not received after a certain time, message will be discarded and the record for C will be deleted. If a node receives a reply message it will computes and verifies the distance to the sender from the received signal and will then compute its distance from C. If distance matches the information in the table it will mark the record as updated. If the node is not the request originator, it will then forward the reply towards V and updating the value of dc with its own. If the distance does not match or is not within an acceptable range criteria (i.e. within physical communication range and road limits). The major drawback in this paper. This scheme is an option for disseminating messages among the vehicles when they are not within the range of transmission. But interference, packet collisions and hidden nodes terminate message dissemination by mediating unwanted re-transmissions over the resources is the biggest challenge in the multi-hop transmission.

Khaled Alodadi et all proposed an Co-operative volunteer protocol[19] to detect NLOS in vehicular ad hoc network. Co-Operative Volunteer Protocol which uses volunteer vehicles to disseminate the warning message from source to target vehicle experiencing an NLOS situation. This uses the concept of Context Aware System (CAS), which clarifies On Board Unit (OBU) component and their interaction with each other to collect data and make decision based on the sensed circumstance. The CVPBDS is used as an efficient mechanism for routing protocol capable of broadcasting warning message from emergency vehicle to vehicle under NLOS condition to reduce the overhead and increase the packet delivery ratio with reduced time delay and channel utilization. This CVP architecture utilizes a five layered Context-aware system to enhance the intelligence, awareness of surrounding events and cost effectiveness of the overall system. The On board unit architecture that is presented in this paper is used in every vehicle, in addition to a Warning Message Byte(WMB),which consists of warning message data packets that inform the system about upcoming emergency events to enable it to response to this event separately. The architecture is a top down approaches consisting of three main phases. First phase represents the sensing layer where raw data is gathered from different components. Second phase is represents by three layers (raw data retrieval, processing and storage unit).Third and final phase is represented in the action layer, where the dissemination units take place.The main contribution of this work is the presentation of new routing management based on the design of a new routing protocol for the detection of NLOS situations on the road at intersections. The work involved distribution of warning messages broadcast by the source vehicle (emergency vehicle) to a target vehicle facing an NLOS situation. In addition, the simulation results demonstrated that CVP achieved the target of the successful dissemination of warning messages to vehicles under NLOS through cooperatively delivering messages to these vehicles, thereby solving the NLOS situation successfully. It has been shown that CVP can operate in two modes: an intersection scenario in which a vehicle is hidden by a bus, truck or building, thereby preventing access to warning messages from the source emergency vehicle to the vehicle hidden by an obstacle; and the highway scenario in which the location of the target node under NLOS is hidden by some other vehicle (bus, truck) or foliage along the highways. CVP effectively detected the NLOS and was triggered to solve the NLOS using the cooperative approach for message delivery to the target vehicle. The CVP proposed in this work was able to outperform GRANT in terms of the ability of CVP to detect NLOS situations by using the RIT data.One of the major drawback in this paper is the utilization of high number of control message for tracking the localization NLOS nodes. The distribution of warning message is difficult if the number of nodes are high in number. The authentication, trustworthy, integrity and acknowledgement may not be provided properly by volunteer vehicle.

Lina Bariahet al proposed an recent advances in VANET security[20]. Vehicular ad hoc network (VANET) are emerging as a prominent form of mobile ad hoc networks (MANETs) and as an effective technology for providing a wide range of protection inquiry for transport passengers. Nowadays, VANETs are of an increasing importance as they enable accessing a large variety of ubiquitous services. Such increase is also associated with a similar increase in vulnerabilities in these inter-vehicular services and transmission, and consequently, the number of security attacks as well as threats. It is defined as the transmission between the transport as well as possibly with the side units, that is, at least one of the transmitting and receiving units is a transport and possibly is routing node. VANET became progressively major and popular in many countries as part of the Intelligent Transportation Systems (ITSs). The fundamental VANET application is to allow any equipped vehicle to broadcast safety messages that are related to status of the road to other nearby transport so that they adjust their traveling routes, as well as to nearby RSUs which will communicate with traffic control center to synchronize traffic lights to decrease road traffic jam, manage emergency and traffic incidents operations, etc., .if a time-critical message sent by an “innocent” vehicle and was intentionally changed, dropped, or re-routed to the wrong receiving unit by an routing “malicious” vehicle, severe consequences will be the outcome (e.g. the innocent vehicle may get accused, possible injuries and deaths, etc). This demands the development of a robust and reliable security measures in VANETs and require intensive and deep studies to help in preventing malicious activities in the network. Authentication and non-repudiation are the two most major necessity for secure VANETs, many security mechanisms have been introduced for the deployment of these security necessity, the most used mechanisms are: Public Key Infrastructure, ID-Based cryptosystem and Situation Modeling-Based mechanism. The major drawback in this paper is if a time-critical news sent by an “innocent” transport and was intentionally modified, discarded, or re-routed to the wrong receiving unit by an routing “malicious” transport.

The advantages and disadvantages of various methods have been summarized in the below table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl.No** | **Author Name and Publication Details** | **Method Name** | **Advantage** | **Drawbacks** |
| 1 | Sven Bauer, Marcus Obst, Robin Streiter and Gerd Wanielik “Evaluation of Shadow Maps for Non-Line-of-Sight Detection in Urban GNSS Vehicle Localization with VANETs—The GAIN Approach”2013. | Evaluation of Shadow Maps for Non Line –of-Sight detection in GNSS vehicle localization with VANET.  | NLOS detection in urban areas. | **GPS specific problems:** Signal reflection due to non-line-of-sight. Full blockage of GPS signal due to buildings or foliages.OSM database does not entirely contain all the informations. |
| 2 | Yumeng Gao, Peter Han Joo Chong*,* Yong Liang Guan” BSM Dissemination with network coded relaying in VANETs at NLOS Intersections”2017. | BSM Dissemination with network coded relaying in VANETs at NLOS Intersections | The Dedicated Short Range Communication supports the applications by broadcasting basic safety messages (BSMs) periodically. RT-NCI and RT-NC are used, to enhance the reliability of BSM dissemination. | RT-NCI is not as reliable as RT-NC because RT-NCI applies the random linear network coding at single relay node |
| 3  | SrdjanCapkun, Mario Cagalj, Ghassan O. Karame “Integrity Regions: Authentication through presence in Wireless Networks” 2015 | Integrity Regions: Authentication through presence in Wireless Networks | Authentication messages can be transferred from devices using the Integrity Regions | When Integrity Region (IR) radius increases, the number of encounters between nodes increases. Therefore an attacker can perform MITM attacks from larger distances, when the IR region grows in size. |
| 4 | Reza Monir Vaghefi, R. Michael Buehrer “Cooperative Source Node Trackingin Non-line-of-sight Environments “2016. | Cooperative Source Node Trackingin Non-line-of-sight Environments | A novel sensor tracking algorithm based on Semi definite programming (SDP) which has the ability to mitigate NLOS propagation. | Semi definite programming (SDP) method runs multiple iterations until the required accuracy is achieved.so it is complexity |
| 5 | Khaled Alodadi, Ali H. Al-Bayatti , Nasser Alalwan “Cooperative volunteer protocol to detect non-line of sight nodes in vehicular Ad-Hoc networks”2017 | Co-operative volunteer protocol to detect NLOS in Vehicular ad hoc network | It is an efficient mechanism for broadcasting messages emergency vehicle to vehicle under NLOS situation | The dissemination of warning message is difficult if the number of nodes are high in number. The authentication, reliability, integrity and acknowledgement may not be provided properly by volunteer vehicle. The utilization of high 6number of control message for tracking the localization NLOS nodes. |
| 6 | Osama Abumansoor and AzzedineBoukerche,”A Cooperative Multi-Hop Location Verification for Non Line Of Sight (NLOS) in VANET “2011. | A cooperative multi hop location verification for NLOS in VANET. | This scheme is an option for disseminating messages among the vehicles when they are not within the range of transmission | This scheme is an option for disseminating messages among the vehicles when they are not within the range of transmission. But interference, packet collisions and hidden nodes terminate message dissemination by mediating unwanted re-transmissions over the resources is the biggest challenge in the multi-hop transmission.  |
| 7. | Lina.bariah, dina.shehada, ehab.salahat, cyeun “Recent advances in VANET security: A survey” in 2015 | “Recent advances in VANET security: A survey” |  Public Key Infrastructure, ID-Based cryptosystem is used to provide security on authentication andnon-repudiation. | If a time-critical news sent by an “innocent” vehicle and was intentionally modified, discarded, or re-routed to the wrong receiving unit by an routing “malicious” vehicle. |

##### **CONCLUSION**

In this paper the merits and demerits of various methods have been discussed. The warning messages from the emergency vehicle must reach the other nodes more accurately on time to avoid fatal accidents. Hence in the future precise localization of NLOS nodes can be done by using mathematical models like hyperbolic methods and meta-heuristic approaches.

##### **REFERENCE**

1. Mishra et al., “VANET security: Issues, challenges and solution”,[International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7731602), 2016.
2. Road Crash Statistics- Association for Safe International Road Travel.

Available:<http://asirt.org/initiatives/informing->road-users/road-safety-facts/roadcrash-statistics

1. Maxim Raya et al., “The Security of Vehicular Ad Hoc Networks”,SASN’05, Nov 7 2005, Alexandria, Virginia, USA, pp. 11-21
2. Global status report on road safety 2018 published by WHO. Available:https://www.who.int/violence\_injury\_prevention/road\_safety\_status/2018/en/
3. National Crime Records Bureau report in 2016.

Available:https://timesofindia.indiatimes.com/india/90-deaths-on-roads-due-to-rash-driving-ncrb/articleshow/61898677.cms

1. Statistics on Intersection Accidents .

Available : https://www.autoaccident.com/statistics-on-intersection-accidents.html

1. ZaydounYahyaRawashdeh et al., “ Communication in Vehicular Network” ,IEEE 2007.
2. M. Dixit et al., “VANET: Architectures, Research Issues, Routing Protocols, and its Applications”, International Conference on Computing, Communication and Automation (ICCCA2016),2016.
3. O Abumansoor et al., “A cooperative multi-hop location verification for Non Line Of Sight (NLOS) in VANET”,[IEEE Wireless Communications and Networking Conference](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5770420) ,2011.
4. R. K. Schmidt, T. Kollmer, T. Leinmller, B. Boddeker, and G. Schafer,Degradation of Transmission Range in VANETs caused by Interference,PIK - Praxis der Informationsverarbeitung und Kommunikation, Special Issue on Mobile Ad-hoc Networks, Vol. 32, Iss. 4, 2009, pp. 224 234.
5. Franciso J. Matinez et al, “Determining the Representative Factors Affecting Warning Message Dissemination in VANETs” Springer Science + Business Media, LLC. 2011.
6. IEEE P802.11p: Wireless access in vehicular environments (WAVE), IEEE Computer Society,2006.
7. Sven Bauer, Marcus Obst, Robin Streiter and GerdWanielik“Evaluation of Shadow Maps for Non-Line-of-Sight Detection in Urban GNSS Vehicle Localization with VANETs—The GAIN Approach”,2013.
8. A.Sorrentino et.al,. “An effective indicator for NLOS, nLOS, LOS propagation channels conditions”, [6th European Conference on Antennas and Propagation (EUCAP)](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6200795), 2012.
9. S. Capkun and M. Cagalj, “Integrity Regions: Authentication through Presence in Wireless Networks,” Proc. ACM Workshop Wireless Security (WiSe ’06), 2006.
10. Reza MonirVaghefi and R. Michael Buehrer, “Cooperative Source Node Trackingin Non-line-of-sight Environments”,2016.
11. O Abumansoor et al., “A cooperative multi-hop location verification for Non Line Of Sight (NLOS) in VANET”,[IEEE Wireless Communications and Networking Conference](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5770420) ,2011.
12. R. K. Schmidt, T. Kollmer, T. Leinmller, B. Boddeker, and Schafer,Degradation of Transmission Range in VANETs caused by Interference,PIK - Praxis der Informationsverarbeitung und Kommunikation, Special Issue on Mobile Ad-hoc Networks, Vol. 32, Iss. 4, 2009, pp. 224 234.
13. KhaledAlodadi, Ali H. Al-Bayatti , Nasser Alalwan“Cooperative volunteer protocol to detect non-line of sight nodes invehicular Ad-Hoc networks”2017.
14. Linabariah et al., “Recent Advances in VANET Security”, [IEEE 82nd Vehicular Technology Conference](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7389774),2015.