A Novel Approach For Security Aware Topological Based Routing Protocol In Vehicular Adhoc Network

A.P. Jadhao, Dr.D.N.Chaudhari

Abstract — Vehicular ad hoc networks (VANETs) have attracted a lot of attention over the last few years. They have become a fundamental component of many intelligent transportation systems and VANETs are being used to improve road safety and enable a wide variety of value-added services. Many forms of attacks against VANETs have emerged recently that attempt to compromise the security of such networks. Such security attacks on VANETs may lead to catastrophic results such as the loss of lives or loss of revenue for those value-added services. Therefore making VANETs secure has become a key objective for VANET designers. To develop and deploy secure VANET infrastructures remains a significant challenge.
In the proposed research work likely focus on the latest research areas in Vehicular Adhoc network. With the help of recent tools and technologies .This research develops and evaluates some of the main security threats and attacks that can be exploited in VANETs and present the corresponding security solutions that can be implemented to thwart those attacks on reactive routing protocol under topological based routing protocol for improving security under possible attacks of VANETs relying on broadcast for sharing safety and road information among vehicles and related attacks. communication characteristics will be developed and evaluated.

Keywords: Performance, Routing protocol, VANET, V2V, V2I.

1.INTRODUCTION

Vehicular ad hoc networking is an emerging technology for future on-the-road communications. Due to the virtue of vehicle-to-vehicle and vehicle-to-infrastructure communications, vehicular ad hoc networks (VANETs) are expected to enable a plethora of communication-based automotive applications including diverse in-vehicle infotainment applications and road safety services. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large-scale VANETs with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative [1]. Via inter-vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated.VANET belong to a general class of mobile ad hoc communication networks with fast-moving nodes (i.e., vehicles). In specific, a VANET consists of (a) on-board units (OBUs) built into vehicles and (b) roadside units (RSUs) [2,3,] deployed along highways/sidewalks, which facilitates both vehicle-to-vehicle (V2V) communications between vehicles and vehicle-to-infrastructure (V2I) communications between

vehicles and RSUs. The impact of mobility models on VANET results, as well as the inadequacy of the mobility models usually adopted in MANET result [3,4]. Each node in the network like VANET [5,6] acts as the host node as well as router node in order to perform the forwarding operation. For the building of the routes and in order to build the network, the mechanism of routing protocols in the VANET networks introduced.
The main functionality of routing protocols is to build the dynamic routes between any source and destination nodes in the network. Network topology for the VANET networks is not fixed because of the frequent nodes movement in the network. According to the movements of the nodes is resulted into the frequent topology changes. There are mainly three types of routing protocols proposed for the VANET routing such as proactive, reactive and hybrid routing protocols [7] and their simulation study with different network scenarios and traffic patterns. DSDV and OLSR [8] are the examples of the proactive protocols, AODV[15] and DSR [33] are the well-known reactive routing protocols and ZRP[2] is one of the hybrids routing VANET protocol. Security is the main concern of these applications where a wrong message (due to insecure environment) may directly affect the human lives. Dedicated Short Range

Communication (DSRC) is used as communication medium and it operates on 5.9GHz frequency band. DSRC is based on IEEE 802.11a standard and IEEE 1609 working group is being standardized as IEEE802.11p for special vehicular communication .

Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships among participating nodes. Nodes have several security problems such as easy to hear, modification, impersonating [12]. Because of these reasons, safe transmitting of packets and specially establishing a method for safe routing are most important challenges in ad hoc network. Many attacks have been identified in ad hoc network most of which concentrate on routing operation. VANETs have their special specifications but they are not immune from security threats.

2. RESEARCH ISSUES IN VEHICULAR ADHOC NETWORKS

There are many research problems that must be solved to support the Vehicular Ad Hoc Networks. Solutions to these problems are needed both in terms of proactive, reactive and hybrid approaches. The solution should comprise of all three components prevention, detection and reaction.

Following security issues and challenges are to be handled in Vehicular Ad Hoc Networks (VANETs):

A. ATTACKS AND THREATS:

I) Denial of Service attack:

This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application's information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles [9].

II) Black Hole attacks:

In these attacks, black hole attack is that kind of attack which occurs in Vehicular Ad-Hoc networks (VANET). In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [10].

III) Wormhole attack:

A particularly severe security attack called the wormhole attack, has been introduced in the context of ad-hoc networks. During the attack, a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. This research argues that the proposed approach is more appropriate to address ad hoc networks' dynamic and cooperative nature especially at the application level. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed vehicles network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality[11].

IV) Replay Attack:

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending . Basic 802.11 security has no protection against replay. It does not contain sequence numbers or timestamps. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the system. Individual packets must be authenticated, not just encrypted. Packets must have timestamps. The goal of such an attack would be to confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents.

V) Sybil Attack:

This attack happens when an attacker creates a large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route. A Sybil attack depends on how cheaply identities can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically[12].

B) VEHECULAR NETWORKS CHALENGES:

I) Mobility

The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection throw their way with another vehicles that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is hard problem.

II) Volatility

The connectivity among nodes can be highly ephemeral and maybe will not happen again. Vehicles traveling throw coverage area and making connection with

other vehicles, these connections will be lost as each car has a high mobility and maybe will travel in opposite direction. Vehicular networks lacks the relatively long life context, so personal contact of users device to a hot spot will require long life password and this will be impractical for securing VC.

III) Network Scalability

The scale of this network in the world approximately exceeding the 750 million nodes and this number is growing another problem arise when we must know that there is no a global authority govern the standards for this network [2] for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe the standards for the GM Vehicles is deferent from the BMW one.

IV) Bootstrap:

At this moment only few number of cars will be have the equipment required for the DSRC radios, so if we make a communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the commercial firms to invest in this technology.

3. LITERATURE REVIEW

Secure routing in VANETs has been of interest for quite some time in the research community. In this section we will give a short overview of existing work and entry points to the literature.

The reason why researchers try to solve the challenge of securing routing protocols are attacks. Many different types of attacks have been proposed so far. A selection of them are Denial of service attack (Dos)[9], Black Hole attack[10], wormhole attack [11].

Hafez Maowad et. al (2012)[13] proposes SD-AOMDV as VANET routing SD-AOMD improves the most important on demand multipath routing protocol AOMDV to suit VANET characteristics. SD-AOMDV add the mobility parameters: speed and direction to hop count as new AOMDV routing metric to select next hop during the rout discovery phase. SD-AOMDV is designed, implemented, and compared with AOMDV. Simulation results show that SD-AOMDV has outperformed AOMDV in city and highway with different traffic scenarios.

Alpana Dahiya et. al (2012)[14] proposed an algorithm to solve the congestion problem in all path network and to get such a path that will provide efficient data transmission over the network. The network is divided into sub-networks and the transmission over the sub goal and to achieve the efficient and reliable data transmission.

Ben Ding et. al (2011)[15] proposed an improved AODV routing protocol using two step optimization in route discovery & route selection process to improve route stability & describe control overhead to achieve better performance in the form of higher packet delivery ratio & fewer broken links. Overall overhead of protocol is less than AODV because the discovery phase is restricted to certain no. of nodes rather than whole network.

Min-Hsuan Wei et. al (2011)[16] presented a simple and reliable routing scheme based on vehicle moving similarity (RR-VMS), which supports stable rebroadcast nodes selection and efficient route discovery to make inter-vehicle data transmissions more reliable. RRVMS uses VPS to reflect the stability of neighbor vehicles. A vehicle with a high VPS, chosen as a rebroadcast node, will stay long enough in an inter-vehicle transmission path. Moreover, to reduce the number of rebroadcast nodes, define a donut-like selection area and restrict the number of rebroadcast nodes to reduce the route hop counts and network traffic. The proposed RR-VMS method can also be applied to other ad hoc routing protocols that involve broadcast.

Won-I Lee et. al (2011)[17] conclude that DSR has better PDF and lesser routing overload than others. In the case of end to end delay AOMDV is performing comparatively better in both two models. Also it shows that reactive routing protocols performance decreases in space graph model. To select a routing protocol for VANET emphasize more on end to end delay performance metric. Results shows that for packet delivery fraction, the difference between routing protocols are not that significant but for end to end delay, the differences are more significant. In VANET, AOMDV is more appropriate than DSR and AODV though AOMDV requires more routing load.

Gongjun Yan et. al (2009)[18] describe a feasible and novel geographic location-based security mechanism for vehicular adhoc network environment .The proposed algorithm is efficient on the basis of simulation.

R.Yu et.al (2011)[19] proposed a general geographical routing scheme called DGIF, based on which we model a WSAN as a controlled stochastic system with disturbances (i.e. uncertain positions of remote nodes). The routing process was studied from the perspective of stochastic optimal control. An improved value iteration method has been proposed to accelerate the convergence of the optimal routing policy. They also proposed a reliability-driven routing algorithm and a QoSaware routing algorithm for various applications.

YUN WEI LIN et.al (2010)[20] surveys existing unicast, multicast, and broadcast protocols for VANETs. The unicast routing protocols are split into min-delay and delay-bound approaches. The min-delay unicast routing protocols construct a minimum-delay routing path as soon as possible. The delay-bound routing protocol utilizes the carry-and-forward technique to minimize the channel utilization within a constrained delay time. The multicast in VANETs is defined by delivering multicast packets from a mobile vehicle to all multicast- member vehicles. The geocast in VANETs is defined by delivering geocast packets from a source vehicle to vehicles located in a specific geographic region. A mobicast outing protocol in VANETs is also described.

S.S.Dorle et.al (2010)[21] introduce a traffic model depending upon the transmission range. The model has taken unicast routing and number of vehicles moving on the lane having their respective speed. As long as the vehicle is in the transmission range the ITS facilities can be utilized. So it is necessary that the maximum range can be made available.

Samina Ehsan et.al (2010)[22] present a comprehensive review on research challenges and the state-of-the art of energy-aware routing techniques for WMSNs, and highlight the advantages and performance issues of each routing protocol and algorithm. Open issues are provided in order to stimulate more research interests in those unexplored areas. It is doubtless that being blessed by the growing advancement of hardware technology, WMSNs will reveal as a powerful technology in near future. Developing efficient routing protocols for WMSNs appears to be a promising direction of future research.

Farzad Sabahi (2011)[23] describe an approach of computing, communications which introduces the benefits of using several kinds of its technology. VANET is a new technology and has considerable vulnerabilities certainly which give great chances to attackers to break it. These malicious users always try to challenge the networks with their selfish behavior. Adhoc protocols play the main role in VANET but they have size limits and are always smaller than the VANETs. The size of VANETs and their characteristics inherited from adhoc make difficulties in implementing security capabilities and policies.

Jorg Buhler et.al(2010)[24] present a state aggregation procedure for the computation of HAM policies which results in a drastic state space (and hence, complexity) reduction. Using the algorithm in a heterogeneous GSM-EDGE/UMTS scenario, obtained the significant performance gains in comparison to the straightforward Greedy Load-based policies. This indicates that the aggregated model, though of greatly reduced state space size, still carries enough information about the problem structure to be able to find good control policies.

Qing Yang and Alvin Lim et.al(2008)[25] presented an algorithm for selecting routes with the highest probability of connectivity and thus avoid network disconnections in VANETs. This algorithm uses a novel model of network connectivity. Because the selection procedure is independent of the number of nodes, this approach is demonstrated to perform well in both dense and sparse networks.

Brijesh Kadri Mohandas et.al(2009)[26] describe the behavior of adaptive PI rate controller while dealing with the problem of vehicle traffic congestion. The adaptive PI rate controller is a potential algorithm to deal with the problem of vehicle traffic congestion as seen when the traffic volume exceeds the road capacity. In practice, the average waiting time could be calculated using the information provided by the algorithm and some intelligence that can calculate the current number of vehicles waiting to use the road segment. Using VANET, this information can be transmitted to prospective drivers before they reach the intersection in order to assist them to choose a congestion free route.

Omid Abedi et.al (2009)[27] proposed DAODV protocol that improves the performance issues on common AODV protocol. The main goal of DAODV is to establish more stable routes especially in the applications that demand high mobility of nodes such as VANETs. The proposed method uses two important parameters of movement (direction and position) to select next hops during route discovery phase. The overhead of each route in AODV is less than DAODV, but the overall overhead of DAODV is less, because its discovered routes have been reduced.

Noppakun Yawan et.al(2009)[28] presents two methods of AODV improvement, which are Channel Availability calculation and Mobility Prediction, by calculating distance change rate. The calculated channel availability and distance change rate is used in an AODV path discovery decision-making process whether to forward incoming RREQ packets or not. If the channel availability value is lower than its threshold and the distance change rate is more than its threshold so the incoming RREQ packets will not be forwarded. This helps AODV to avoid routing in a dense communication channel and to increase a route lifetime such that it can decrease delay and increase transmission reliability.

Wenjing Wang et.al(2007)[29] propose a two-phase routing protocol, and address the packet routing issue similar as a vehicle moving on a map. In TOPO, packets are routed along a pre calculated path in high traffic density roads, together with local area routing support. The proposed TOPO protocol can be also regarded as a framework in large scale VANET routing that is compatible with various single-stage routing protocols

Xi Yu et.al(2011)[30] proposes the new routing protocol AODV-VANET by incorporating the vehicles movement information into the route discovery process based on AODV for VANET application. With the introduction of the TWR and expiration time estimation, the proposed protocol is able to achieve better routing performances.

Han Guo et.al(2011)[31] introduced framework, the main function of the information processing applicaton module is collecting the real-time traffic datum from the road network, analyzing and dealing with them. To insure the system work normally and safely, the researchful task of security is crucial.

D.Sutariya et.al(2012)[32] proposed verify IAODV improvement for other type of road topologies because in real world road topology is different for different areas of city and highways. The DSRC standard is adopted by ASTM and IEEE to provide a secure, reliable, and timely wireless communication component as an integral part for the intelligent transportation system (ITS) by supporting multichannel communication.

S. S. Manvi et.al (2009) [33] describe the routing protocols AODV, DSR, and SWARM, and analyzed the

differences in their performance. These performance evaluations are necessary to devise the new routing protocols for VANETs. An important observation was that the examined routing protocols showed highly heterogeneous performance results.

S. Mohammad Safi et.al (2009) [34] proposed a scheme which can be performed easily in AODV protocol with low overhead, no requirement of any special hardware and without any complex calculation.The proposed method, used geographical leashes after a correction on it. Also we used HEAP for safety of control packets (naturally packet leashes parameters) and traffic packets. The method created have low overhead for network while it secured it against wormhole and can detect malicious nodes as far as possible. The proposed method can easily be used for all VANTE applications regardless of whether the message transfer is unicast, broadcast or multicast and it secures this type of network against wormhole attack.

Jianping Wanget.al (2009) [35] adopt the principle of sequence number increment to judge the credibility of the route for the following packets. But it is not the sole criterion whether the sequence number is followed by the strict increment. In some condition, such as some nodes' high-speed mobile and less demanding on the security, we can set the threshold value (E.g. the difference between two sequence numbers can't be larger than 10) as the criteria of credibility division.

4. THE PROPOSED WORK

From the study of aforementioned related work in the field of security issues concerning routing protocols for VANETs and from the review of current literature [following research problems have been identified.

- Methods and tools for evaluation of VANET routing protocols.
- To implement mobility model for VANET.
- To implement the communication types in VANET.
- To develop multilevel solution for messages within RSU range.
- To perform extensive analysis of the proposed system.
- An improved Topological based VANET routing protocol.
- Characterize different topological based VANET routing protocols and locate the factors that affect control overhead
  - ❖ Predict trends of control overhead when the network environment changes
  - ❖ Improve existing routing protocols with emphasis on control overhead

This research work is an attempt to address all or few of the problems mentioned above. The broad scope of the proposed work is Computer Networks under the field of Computer Science & Engineering. The proposed research is aimed at innovation in the design of secure topological based routing protocols for VANET.

5.METHODOLOGY

As Research Methodology is a way to systematically solve the research problem. This research develops and evaluates some of the main security threats and attacks that can be exploited in VANETs and present the corresponding security solutions that can be implemented to prevent those attacks on reactive routing protocol under topological based routing protocol. This Involves

- Implementation of topological based reactive routing protocol AODV, DSR and performance analysis will be examined under different parameter packet delivery ratio, average end-to-end delay and normalized routing overhead.
- Implementation of different attack on reactive routing protocol and examine the network under different scenario.
- Implementation of secure routing protocol and examine the network under different scenario and comparison of the proposed system with the existing system.

The adopted methodology for the results of this research work will increase security. This research investigates various implementation issues of VANETs, simulation and analysis of the existing Privacy system. Communication channel models for outdoor environment of VANET. Indentify the various parameters that are significant in the implementation of location base VANET privacy system. Modification in the existing location base VANET privacy system for improved performance multilevel communication channel. Development of the mathematical model of the proposed system. Validation of the performance of the proposed system.

6. Research Plan

The Research study is expected to arrive at some approximation of scientific truth through these steps: 1) A comprehensive search of existing knowledge on the topic found through a literature review. 2) A rigorous and well-formulated methodology that provides sound logic for arriving at the intended results. 3) Design of algorithms & Preparing Research Design, which includes a precise form of data collection. 4) Determining the results, including an appropriate form of statistical analysis of the data 5) Discussion that summarizes the results relative to the originally stated hypotheses and the existing body of relevant knowledge on the subject and 6) Preparation of Thesis.

7. IMPLICATIONS

Here, primary focus is on implementing a new efficient scheme in topological based routing protocol for Vehicular ad hoc network. The development of secure topological based routing protocol helps to develop intelligent networking system to increase throughput.

The motivation for future network will need to manipulate precious information with a possible impact on driver behavior and even on human life. Therefore, any solution needs to be thoroughly tested before integration in a real system. Field tests require not only implementation of the solution on real hardware, but also dedicated road infrastructure and equipped vehicles. Even the large-scale deployment scenarios that are currently prepared will only have the capacity to test a minor proportion from the proposals made by the VANET research community.

On the other hand, the vehicular environment is highly complex and analytical models need to take into consideration not only the network, but also the properties of the vehicles and the behavior of the drivers simple traffic models are inappropriate for road traffic simulation, the impact of IVC on road traffic can be directly evaluated.

The proposed research fulfills the requirement of privacy technique for location based and working for RSU unit. However, these solutions still require precise topological information like building location. VANET simulation is the large number of nodes that need to be modeled. This is because in a wireless simulation, the receivers need to be searched among all the other entities and gives support to secure communication. Meanwhile, our proposed solution will provide security for different attacks that does not require support from the roadside infrastructure or the OBUs is secure against adversary.

REFERENCES

1. Ho Ting Cheng, et.al,"I*nfotainment and road safety service support in vehicular networking: From a communication perspective* ", www.elsevier.com/locate /jnlabr/ymssp, (2011) / page no. (2020–2038) /doi:10.1016/j.ymssp.2010.11.009

2. Hannes Hartenstein, "*A Tutorial Survey on Vehicular Ad Hoc Networks* ",IEEE Communications Magazine June 2008/ page no.(164-171)

3. A. Shastri et.al,"*Performance Analysis of on-demand routing protocol for Vehicular Ad-hoc Networks"*, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011 DOI : 10.5121/ijwmn.2011.3407 page no.(103-111)

4. Josiane Nzouonta,et.al*,"VANET Routing on City Roads Using Real-Time Vehicular Traffic Information*", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009 page no.(3609-3626)

5. Boangoat Jarupan , et. al "*A survey of cross-layer design for VANETs*",
Ad Hoc Networks 9 (2011) page no (966–983),www.elsevier.com/locate/adhoc

6. YASSER TOOR, et al."*Vehicle Adhoc Networks: Applications And Related Technical Issues*",IEEE COMMUNICATIONS 3RD QUARTER 2008, VOLUME 10, NO. 3 page no (74-87).

7. Jinyuan Sun, et.al,*,"Location-Based Secure and Dependable VANETs for Disaster Rescue*", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011 page no (659-669).

8. Sherali Zeadally, et. al ,"*Vehicular ad hoc networks (VANETS): status, results,and challenges*", Springer Science 2010

9. Halabi Hasbullah,"*Denial of Service (DOS) Attack and Its Possible Solutions in VANET"*, World Academy of Science, Engineering and Technology 41 2010 page no (411-415).

10. Vimal Bibhu, et. al **,"***Performance Analysis of Black Hole Attack in Vanet",* I. J. Computer Network and Information Security, 2012, 11, page no (47-54).

11. Harbir Kaur, et. al,"*An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks"*, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, 2012 page no (86-89).

12. Gilles Guette et. al *,"On the Sybil attack detection in VANET"*, 1-4244-1455-5/07/ 2007 IEEE

13. Hafez Maowad et. al ,"*Efficient Routing Protocol for VehicularAd Hoc Networks*", page no(209-215)/ 2012 IEEE

14. Alpana Dahiya et. al **,"***Path Discovery In Vehicular Ad hoc Network",* 2012 Second International Conference on Advanced Computing & Communication Technologies / 2012 IEEE /DOI 10.1109 /ACCT.2012.83/ page no.(551-555).

15. Ben Ding et. al"*An Improved AODV Routing Protocol for VANETs*" 978-1-4577-1010-0/11/ 2011 IEEE.

16. Min-Hsuan Wei,"*A Reliable Routing Scheme Based on Vehicle Moving Similarity for VANETs*", 978-1-4577-0255-6/11/page no.(426-430)/2011 IEEE.

17. Won-Il Lee et. al *,"Performance Evaluation of Reactive Routing Protocols*

in VANET", 2011 17th Asia-Pacific Conference on Communications (APCC) 2nd – 5th October 2011 IEEE page no (559-564).

18. Gongjun Yan, et. al*,"An Efficient Geographic Location-based Security Mechanism for Vehicular Adhoc Networks*",978-1-4244-5113-5/09/page no (804-809)/2009 IEEE.

19. R. Yu*,"Distributed geographical packet forwarding in wireless sensor and actuator networks – a stochastic optimal control approach*", IET Wirel. Sens. Syst., 2012, Vol. 2, Iss. 1, page no(63–74) 63 doi: 10.1049/iet-wss.2011.0093.

20. YUN-WEI LIN*,"Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives*", JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 26, page no (913-932) (2010).

21. Sanjay S. Dorle*,"Wireless Transmission Impact on the Lifetime of Routing Path in VANET"*, 978-0-7695-4246-1/10/ page no(101-105) 2010 IEEE DOI 10.1109/ICETET.2010.117.

22. Samina Ehsan et. al ,"*A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks",* IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 2, SECOND QUARTER 2012 page no.(265-278).

23. Farzad Sabahi,"*The Security of Vehicular Adhoc Networks*", 978-0 -7695-4482-3/11 2011 IEEE DOI 10.1109/CICSyN.2011.77/ page no.(338-341).

24. Jorg Buhler*,"Traffic-Aware Optimization of Heterogeneous Access Management"*, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 58, NO. 6, JUNE 2010 page no.(1737-1747).

25. Qing Yang et. al,"*Connectivity Aware Routing in Vehicular Networks"*, 1525-3511/08/2008 IEEE page no.(2218-2223).

26. Brijesh Kadri Mohandas*,"Vehicle Traffic Congestion Management in Vehicular ad-hoc networks*", 978-1-4244-4487-8/09/2009 IEEE page no.(655-660).

27. Omid Abedi*,"Enhancing AODV Routing Protocol Using Mobility Parameters in VANET",* 978-1-4244-1968-5/08/2008 IEEE page no.(229-235).

28. Noppakun Yawan et. al*,"AODV Improvement for Vehicular Networks with Cross Layer Technique and Mobility Prediction*" , 978-1-4577-2166-3/11/ 2011 IEEE.

29. Wenjing Wang et. al*,"TOPO: Routing in Large Scale Vehicular Networks*", 1-4244-0264-6/07/2007 IEEE page no.(2106-2110).

30. Xi Yu,"*A Reliable Routing Protocol for VANET Communications*", 978-1-4577-9538-2/11/2011 IEEE page no.(1748-1753).

31. Hang guo et. al*"Research of Security for Vehicular Ad Hoc Networks*" 201O International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), 978-1-4244-7956-6/1 0/2010 IEEE page no.(144-147).

32. D.Sutariya et. al*"An Improved AODV Routing Protocol for VANETs in City Scenarios",* IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012 page no.(575-581).

33. S. S. Manvi et. al *"Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols In Vehicular Ad hoc Network Environment"* 2009 International Conference on Future Computer and Communication, 2009 IEEE page no.(21-25).

34. S.Mohammad Safi,"*A Novel Approach for Avoiding Wormhole Attacks in VANET"*,2009 IEEE.

35. Jianping Wang et. al,"*A Secure DSR Protocol Based on the Request Sequence-Number"*, 978-1-4244-3693-4/09/2009 IEEE.