International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Achieving Fast Communication Mechanism by Using Transitive Trust Relationships for VANET

Venkatatamangarao Nampally[1], Dr. Raghavendra Sharma[2]

[1]Department of Computer Science, University College of Science, Hyderabad, Telangana, India
[2]Department of Statistics, University College of Science, Saifabad, Hyderabad, Telangana, India

ABSTRACT

Vehicular ad hoc networks (VANETs) are a quite prominent research area in the past a few years. One of the main problems of the Vehicular Ad Hoc Networks (VANETs) is achieving fast communication among the established total network. Therefore, achievements are not only reliable data delivery but also the fast authenticity and reliability. In the paper, we present how to obtain the fast communication in VANET system by using Transitive Trust Relationships concept and thus improving the performance of the authentication procedure of the whole network. Moreover, we implement TTRs in NS2 simulator. NAM is used for display the simulation results.

Keywords: VANET, TTRs, NS2, NAM, On-Board-Unit, Road Side Unit, AS, LE, MV, TV, and STDMA.

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is a growing technology in which the vehicle nodes act as routers by using wireless medium to communicate with other nodes in their radio coverage. Vehicular ad hoc networks (VANETs) are a kind of mobile ad hoc network developed to enhance traffic safety and provide comfort applications to drivers. A vehicular ad-hoc network (VANET) is neither restricted geographical area, nor it can be predictable due to its highly dynamic characteristics and requirements. VANET is a term used to describe the spontaneous ad hoc network formed over vehicles moving on the roadside. STDMA algorithm is already in commercial use in the system called automatic identification system. VANET is a network of vehicles and infrastructure points. Vehicles in VANET should incorporate the basic set of sensors such as front and rear radar that receive extra information from surroundings and positioning systems such as the Global Positioning System (GPS) are also found essential for drivers for getting assistance. In modern era, a smart vehicle should be equipped with a communication system with potentially multiple interfaces, a central computing system, an Event Data Recorder (ERD) so that an intruder cannot obtain information and a Tamper Proof Device (TPD). VANET uses a hardware known as TPD to provide security to nodes in communication process. The primary goal of VANET is to provide Road safety conditions to drivers as well as passengers in emergencies.

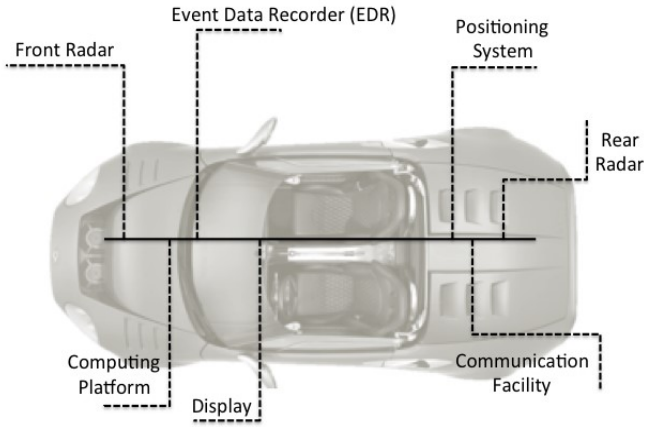

Figure 1. Vehicle components in VANET

The unique features of VANETs include fast moving vehicles that follow pre-determined paths i.e., roads and messages with different priority levels. VANET system domains categorized into, the vehicle domain, the mobile device domain and the infrastructure domain. The vehicle domain comprises all kinds of vehicles such as cars and buses. Using the on-board

unit i.e. node, vehicles can communicate among themselves and with roadside units. The mobile device domain comprises all kinds of portable devices like personal navigation devices and smartphones. In addition, infrastructure domain contains all types of infrastructure used in VANET system. Within The roadside infrastructure domain, there are roadside unit entities like traffic lights. The central infrastructure domain contains infrastructure management centres such as traffic management centres (TMCs) and vehicle management centres. In VANET, system common ccommunication standards are IEEE 802.11p, IEEE1609. In VANET system, vehicles divided as an LE, a MV and a TV. Communication types in VANET system divided as: V2I, and V2V. Internet Engineering Task force (IETF) defined MIPv4/v6 (Mobile Internet Protocol version4/6) and FMIPv6 (Fast) as mobility techniques.

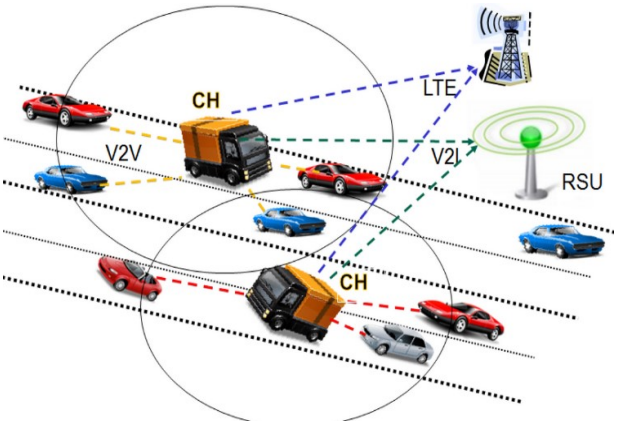

Figure 2. Communications in VANET

If there is successful communication among vehicles then it is V2V communication otherwise, it is to be V2I communication.

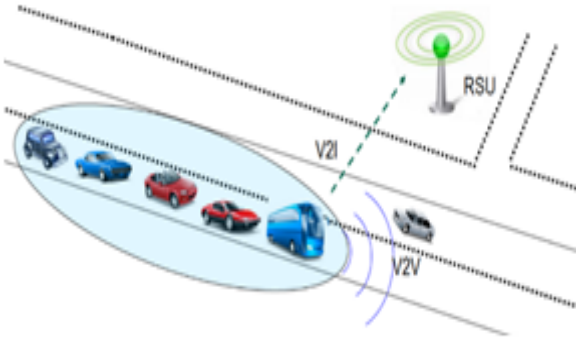

Figure 3. Vehicles communication in VANET

In order, to achieve fast communication in whole VANET, we use Transitive Relationship concept which is wonderful and prominent concept proposed by Ming-Chin Chuang and J.-F. Lee [25]. Trust in computer science defined as a degree of subjectivity belief about the behaviour of a particular entity.

A) Trust characteristics

Trust should be establish based on potential risks; it should be context depended; it should be depend on each party's own interest. The relationship between trust, trustworthiness, and risk figured as:

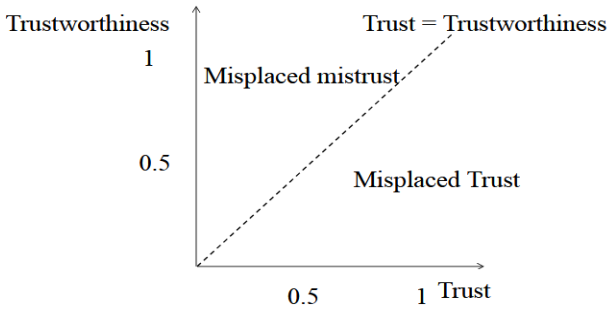

Figure 4. Communications in VANET

Trust in MANET is dynamic, and subjective.

B) Trust management approaches

1) Policy based trust management
2) Reputation based trust management
3) Evidence based trust management
4) Monitoring-based trust management
5) Hierarchical vs. distributed

In MANET Trust management obtained by

1) Secure routing
2) Authentication
3) Access control
4) Key management
5) Transitive trust relationships and
6) General level identification

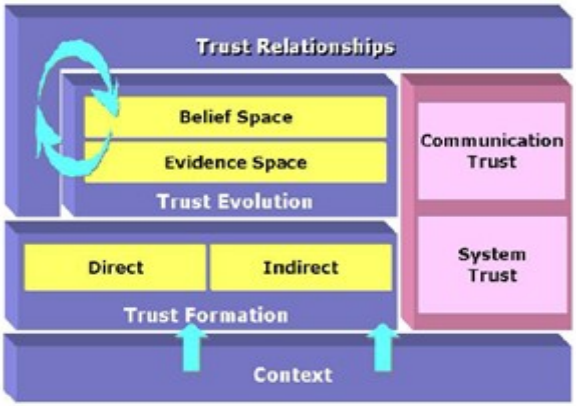

Figure 5. Transitive trust relationships

The remainder of this paper organized as follows:
Section II contains a review of related work. Section III explains problem statement, section IV gives methodology. In Section V, we give the simulation results. In section VI, we give conclusion. In section VII, we give acknowledgment and at last, references given in Section VIII, which used for preparing this paper.

II. RELATED WORK

Existing vehicle-to-vehicle safety systems together with new cooperative systems using wireless data communication. Between vehicles, which can potentially decrease the number of accidents on the highway, road.It observed that one of the main problems of VANET is, getting slow communication among vehicles. It Means, achieving fast communication among nodes in VANET is must in order to overcome that problem. Therefore, in order to achieve fast and secure communication many schemes emerged by using many methodologies. Zhang [7] proposed a RSU-based message authentication scheme, which uses the symmetric key hash message authentication code, instead of a PKI-based message signature, in order to reduce the signature cost. Gowtham [17] achieved communication between nodes takes place in secured way by using security algorithms similar to ECDSA and TESLA. ECC [23] method by Menezes, S. Vnstone, and D. Hankerson achieves best security but low communication latency. So, Ming-Chin Chuang and J.-F. Lee [25] proposed Trust Extended Authentication Mechanism by using XOR operation and TTRs concept .

III. PROBLEM STATEMENT

It is necessary to bring the smart technologies in the ad hoc network environment for achieving efficient and reliable methods for fast data communication, Trust concept well studied in social networks. Golbeck observes social networks as platforms to build mutual trust between entities. However, trust concept in a social network and among infrastructure are different issues. Until the TTR concept introducing, not much work done for obtaining the fast communication for VANET. Therefore, to overcome slow communication problem in VANET system among vehicular nodes, we use Transitive Relationship concept. An enhancement of FMIPv6, a handover management technique used for simulation in a VANET scenario.

IV. METHODOLOGY

Generally, In VANET system all vehicles before communication should be authenticate by a LE. Then only it can able to give authentication to nearby vehicle. This process establishes VANET environment quickly and gives short communication time among vehicular nodes in VANET thus results in increasing the communication capability.

A) Transitive Trust Relationships

In Vehicle-Vehicle communication networks, communication possible among vehicular nodes. A LE authenticate nearby mistrustful vehicle into a trustful vehicle. As the number of LEs are finite, an LE is not always near to the OBU. Even if the user is well meaning, the Vehicle must still wait for the nearest LE and then perform the authentication procedure. Hence, there is an urgent need for an efficient and a reliable communication mechanism. To overcome this process, we follows transitive trust relationships. Let us consider that initially, there are three vehicles in a VANET system. A trustful vehicle (LE) and two other MVs carrying OBUs.

Step 1) the state of the first mistrustful OBU becomes trustful and obtains the sufficient authorized authenticated parameter to authenticate the other mistrustful OBUs when it authenticated successfully with a LE. Then, it plays the temporary LE role and able to give the capacity of authentication to nearby mistrustful node.

Step 2) then this OBU gives authentication to nearby vehicle and makes it into trustful vehicle i.e. temporary LE.

Step 3) then that turning OBU can make change the mistrustful vehicle into trustful.

This mechanism continues to establish big size VANET. This mechanism shown in the following figure.

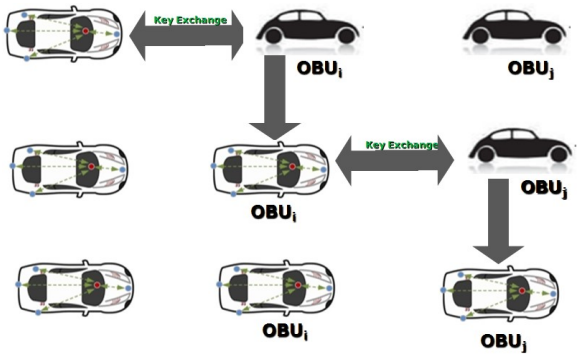

Figure 6. Transitive trust relationships

Thus, the other mistrustful OBU can be authenticated by any trustful OBU without necessarily finding an LE, and all vehicles in a VANET can complete the authentication procedure quickly, In order to forming fast communicated VANET system.

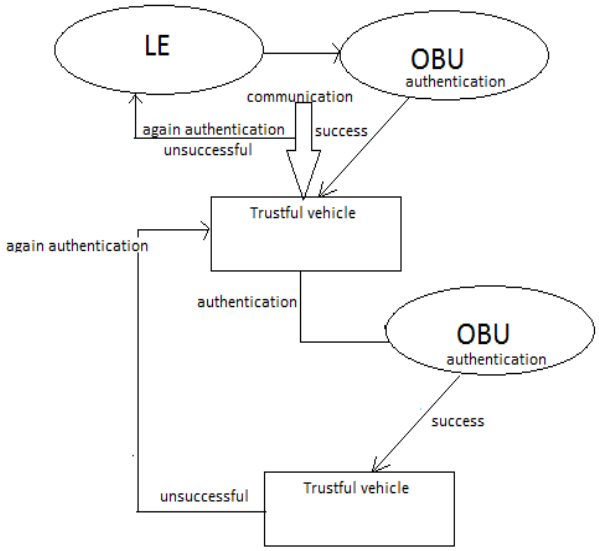

Figure 7. Flow chart of VANET TTRs operations

V. METHODOLOGY

NS2 is the simulating tool for analysing performance of network environment i.e. a network simulator predicts the behaviour of a computer network environment and it gives accurate understanding of system behaviour. It designed specifically for research in computer communication networks. Moreover, the network simulator is the bank of different network and protocol objects. NS2 is one of the most popular simulators used in network research. It is open source and freely available software and developed at the University of Berkeley. It is available for platforms FreeBSD, Linux, SunOS/Solaris, MAC OSX and all windows versions. In ns2 simulator, network protocol stack is written in C++ language for fast to run, OTCL for fast to data write in order to differentiate control and data path implementations. TCL scripting language writes for specifying scenarios, traffic patterns and events. Simulations of VANET often involve large and heterogeneous scenarios.

A. Software Implementation

In implementing Transitive Trust Relationships, we used notepad++ for editing code, which is in Tool Command Language script, Network simulator version 2, windows 7 operating system and XWin Server instead of bash shell. NAM [21] abbreviated for Network AniMator and it is used as a visualization tool for packet level animation. Nam is a TCL/TK animation tool for viewing network simulation traces and real world packet traces. Nam began at LBL.

B. TTRs Screenshots

Transitive Trust Relationships can be achieve in different ways by using different algorithms.

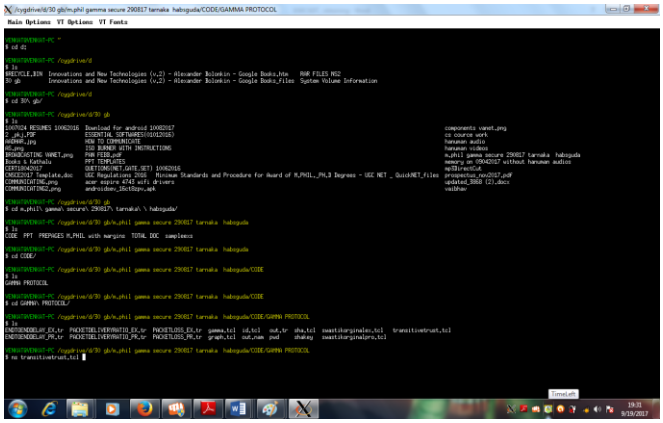

Figure 8. Opening source file of VANET TTRs

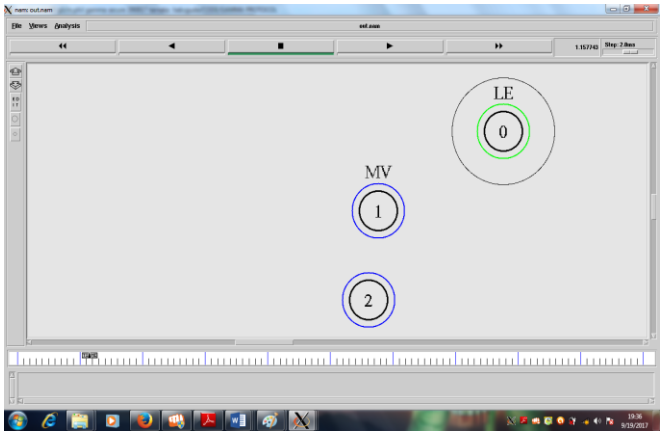

Figure 9. An LE and MVs before communication starts

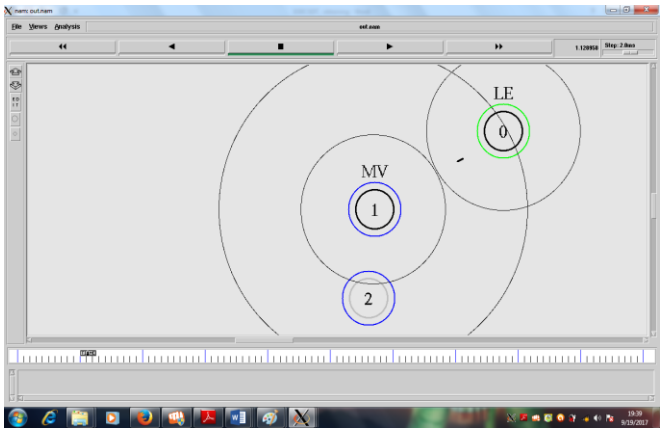

Figure 10. An LE communicating with a MV

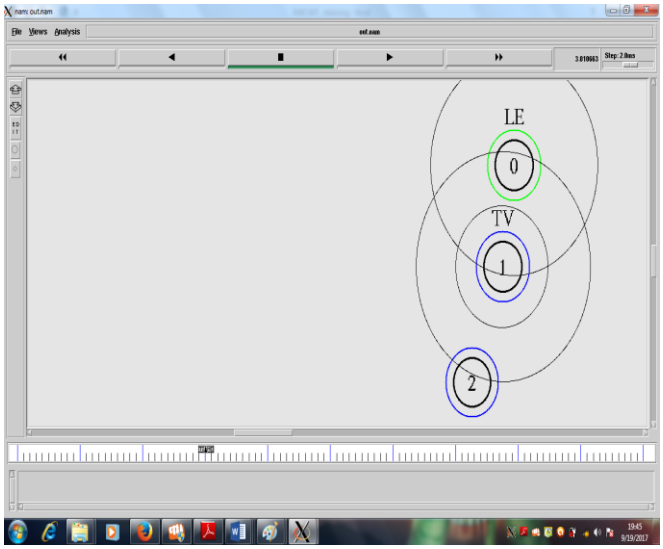

Figure 11. After successful authentication that mistrustful vehicle turns into trustful vehicle

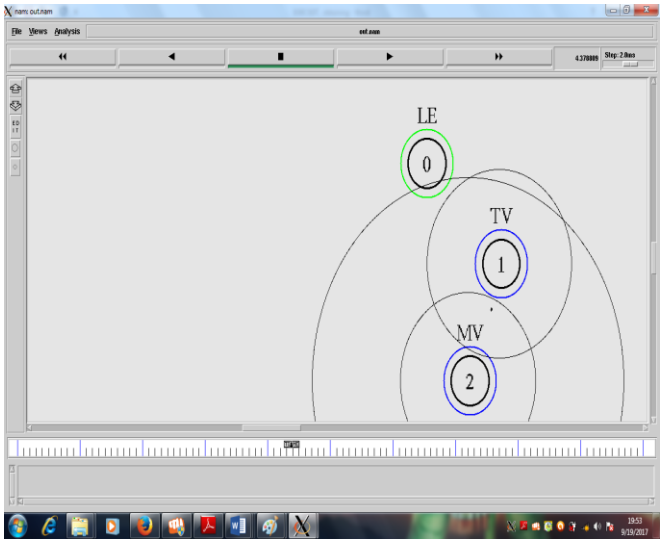

Figure 12. Turned TV giving authentication to another MV

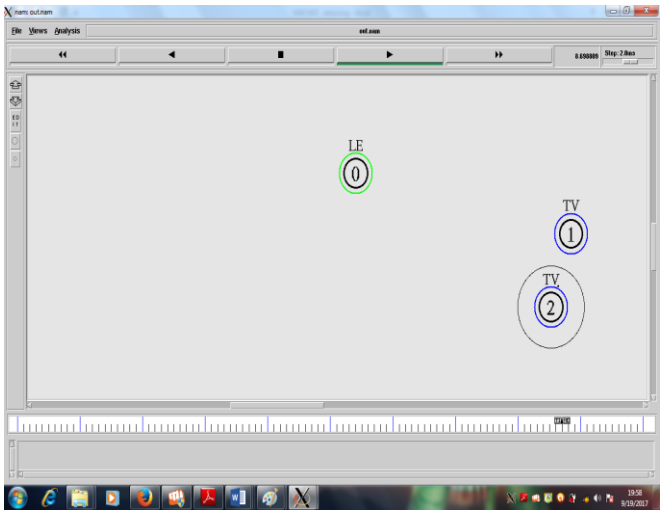

Figure 13. At last, that MV turned into TV

Thus, whole network will be change into trustful environment from mistrustful environment. Here, notice that we can achieve TTRs by using different algorithms.

VI. CONCLUSION

It concluded that for obtaining fast communication in VANETS, we use the TTR concept and thus we achieve fast communication mechanism in VANET system. In this paper, we studied the TTR concept for giving fast communication requirements to the VANET system based on the concept of transitive trust relationships to improve the performance of the authentication procedure. Confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data.

VII. ACKNOWLEDGMENT

I will be thankful forever to the LORD BAJARANGBALI for his boundless blessings showered on me. I am very grateful and express my heartfelt countless Namaste to most respectable and my M.Phil. guide and supervisor who are **Dr. S. Anathi madam ji, B.E.,M.Tech.(IISC),Ph.D., Associate Professor, Department of Network Systems and Information Technology, University of Madras, Guindy Campus, Chennai** for their constant support, invaluable and inspiring guidance to the progress of my paper work. Without madam ji, and Sir K. Padmanabhan inspiration, definitely this paper work would not have been possible.

I would like to express my heartfelt special thanks to most respectable, emeritus and senior **Prof. (ret.) K.Padmanabhan, Former Head, CISL and Emeritus Professor in AC Technology College, Anna University** for their kind support to me for carrying out this paper work.

I would like to express special thanks to **Prof. (ret.) Ramana Murthy M. V., Department of Mathematics & Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, Prof. (ret.) Shankar B., Department of Mathematics, University College of Science, Osmania University, Hyderabad, Telangana** and **R.K.sir** for clarifying my doubts On NS2 software to run on windows 7.

And I take this opportunity to express my heartfelt thanks to **Dr. K.R.Balaji (Guest lecturer in department of NS & IT, University of Madras, Guindy Campus, Chennai) M.Sc.,M.Phil.,Ph.D., Arun Ananthanarayanan, UGC research scholar, Department of NS & IT, University of Madras, Guindy Campus, Chennai** for giving their constant support and valuable help.

Finally, thank you very much **Dept. of NS & IT Scholars**!

VIII. REFERENCES

[1]. M. Raya and J. P. Hubaux, "Securing Vehicular ad hoc networks ," J. Compute. Security, vol. 15, no. 1, pp. 39-68, 2007.

[2]. "time-consuming." Synonyms.net. STANDS4 LLC, 2017. Web. 19 Sep. 2017. <http://www.synonyms.net/antonyms/time-consuming>.

[3]. Yaseer Toor et al., "Vehicle Ad Hoc Networks:Applications and Related Technical Issues", IEEE Communictions Surveys & Tutorials, 3rd quarter 2008, vol. 10, no. 3, pp.74-78.

[4]. Maxim Raya et al., "The Security of Vehicular Ad Hoc Networks," SASN'05, Nov 7 20005, Alaxandria, Verginia, USA, pp. 11-21.

[5]. Dedicated Short Range Communications (DSRC) Online. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[6]. http://www.mdpi.com/2224-2708/5/1/3/htm

[7]. J. P. Hubaux, S. Capkun, and J.Leo, "The security and privacy of smart vehicles," IEEE Security Privacy Mag., vol. 2, no. 3, pp. 49-55, May-Jun. 2004.

[8]. M. Nekovee and B. B. Bogason, "Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks," in Proc. IEEE Vehicular Technol. Conf., Apr. 2007, pp. 2486-2490.

[9]. C. Zhang, X. Lin, R. Lu and P.-H. Ho, "RAISE: An effiient RSU—aided message authentication scheme in vehicular communication networks," in Proc. IEEE Int. Conf. Commun., May 2008, pp. 1451-1457.

[10]. http://slideplayer.com/slide/9398450/

[11]. Jose Maria de Fuentes, Ana Isabel Gonzalez-Tables, and Arturo Ribagorda , "An Overview of Security issues in Vehicular Ad Hoc Networks," Handbook of Research on Mobility and Computing, 2010.

[12]. Mousafa. H, Zhang. Y, "Vehicular Networks:Techniques, Standards, and Applications," CRC Press, (2009).

[13]. Dahill, B. N. Levine, E. Royer and Clay Shields, "A Secure Routing protocol for Ad Hoc Networks," Proceedings of IEEE ICNP 2002, pp. 78-87, Nov. 2002.

[14]. P. Papaadministrators and Z. J Haas, "Secure Data Transmission in Mobile Ad Hoc Networks," ACM Workshop on Wireless Security, San Diago, CA, September 2003.

[15]. J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering o the road: A new data dissemination paradigm in vehicular ad hoc networks," IEEE Trans. Vehicular Technol. Vol. 56, no. 6, pp. 3266-3277, Nov. 2007.

[16]. Kevin Fall, Kannan Vardhan, "The ns manual," The VINT project, December 2008.

[17]. Brent Welch, "Practical programming in TCL and Tk," Prentice Hall, May 1994.

[18]. Vehicle Safety Communications Project, Final Report, DOT HS 810 591, April 2006.

[19]. www.roadtraffic-technology.com

[20]. G.Gowtham , E.Samlinson, "A Secured Trust Creation in VANET Environment Using Random Password Generator," International Conference on Computing, Electronics and Electrical Technologies ICCEET. PP:781-784, 2012.

[21]. www.researchgate.net

[22]. Shyr-Long Jeng, Wei-Hua Chieng, and Hsiang-Pin Lu, "Estimating Speed Using a Side-Looking Single-Radar Vehicle Detector," IEEE transactions on intelligent transportation systems, volume 15, No. 2, (2014).
[23]. H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," IEEE Wireless Commun. Vol. 16, no. 4, pp. 16-22, Aug.2009.
[24]. http://www.isi.edu/nanam/ns/tutorial/index.html
[25]. http://www.nile.wpi.edu/ns
[26]. Menezes, S. Vnstone, and D. Hankerson, "Guide to elliptic curve cryptography," Spinger Professional Computing (Springer, New York 2004)
[27]. Sirwan A Mohammad and Dr. Sattar, "Design of wireless network based on ns2," Journal of Global Research in Computr Science, vol. 3, no. 12, pp. 1-8, (2012)
[28]. http://iitkgp.vlab.co.in/?sub=38&brch=121&sim=561&cnt=1
[29]. http://www.tutorialsweb.com/ns2/NS2-1.html