DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4661
ISSN No. 0976-5697
Volume 8, No. 8,September-October 2017
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

INVENTION OF GAMMA PROTOCOL FOR VANET USING MODULAR ARITHMETIC TECHNIQUES

Venkatamangarao Nampally
Ph. D. Scholar
Department of Computer Science
University College of Science, Osmania University
Hyderabad, Telangana, India

Dr. S. Ananthi
Associate Professor and HOD
Department of Network Systems & Information Technology
University of Madras, Guindy Campus, Chennai
Tamil Nadu, India

Dr. K. Padmanabhan
Emeritus Professsor
Anna University, Chennai
Tamil Nadu
India

Dr. M. Raghavender Sharma
Assistant Professor and HOD
Department of Statistics,
University College of Science, Saifabad, Hyderabad
Telangana, India

Dr. K. R. Balaji &Arun Ananthanarayanan
Department of Network Systems & Information Technology
Guindy campus, University of Madras, Chennai
Tamil Nadu, India

J. Rama, Ph. D. Scholar
Department of Network Systems & Information Technology
Guindy Campus, University of Madras, Chennai
Tamil Nadu, India

Abstract: Vehicular Ad Hoc Networks (VANETs) are the promising approach to provide traffic, safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. Moreover, the security of vehicular ad hoc networks (VANETs) has been receiving a significant amount of attention in the field of wireless mobile networking because VANETs are vulnerable to malicious attacks. Proposed Gamma protocol not only adapts the concept of Transitive Trust Relationships but also improves the performance of the authentication procedure and it provides fast communication with good security than other existing systems. NS2 is open source and discrete event-driven, object-oriented and freely available simulation tool to simulate and analyse dynamic nature of communication networks; it is also a powerful tool to develop new protocols and functions. It provides support for OSI and TCP/IP protocols stack and many standard routing and application protocols for wired and wireless networks. NAM is used to display the process of simulation. We implement Gamma protocol in NS2 Simulator.

Keywords: Ad Hoc Network, VANET, TTRs, GPS antenna, and OSI, TCP Protocol Stack.

1. INTRODUCTION

VANET is a network of vehicles and infrastructure points. It consists of number of reliable sensors within it for communication. The primary goal of VANET is to provide road safety conditions to drivers as well as passengers in emergency situations [1]. In VANET, a modern vehicle communicative parts are as follows:

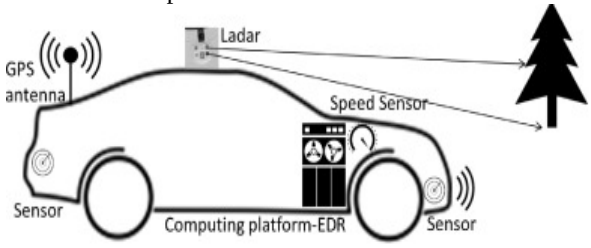

Figure 1. A Modern Vehicle Communicative Parts.

A major drawback of VANET is achieving data dissemination and fast communication [12] so that computation cost and storage space is low. In order to decrease drawback in VANET, many schemes emerged [1]-[15]. Unfortunately, all these schemes lead to high storage cost with slow communication. So, to achieve fast communication, we propose a scheme called Gamma Protocol by using modular arithmetic techniques. The architecture of VANET [3] consists of mainly OBUs (On-Board Units) and RSUs (Road Side Units).OBUs are installed so that each vehicle communicate with each other by using authentication point or RSU. GPS antenna is used for obtain information about places and traffic details. Base stations are deployed in order to access the information. According to the IEEE 802.11p the communication among vehicles can be classified as: V2V and V2I. If there is communication among vehicles then it is said to be V2V, and if there is communication among vehicles and infrastructure then it is V2I. In VANET a base station is not dynamic, so in order to achieve authentication among all vehicles we use Transitive Trust Relationships concept which is very important concept in VANET.

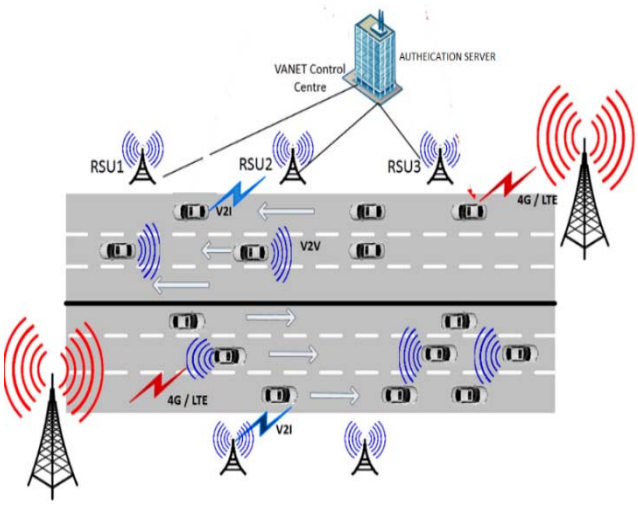

Figure 2. Architecture of VANET [16].

In VANET, vehicles can be classified as [19]:
(1) LE (Law Executor): It can authenticate nearby normal vehicles. It will always act as a permanent TV.
(2)MV (Mistrustful Vehicle): If communication between LE and normal vehicle, then normal vehicle will be turned into TV, otherwise it will be as MV. A MV is nothing but a normal vehicle.
(3) TV (Trustful Vehicle): If communication is successfully existed between LE and MV then it is said to be a TV.

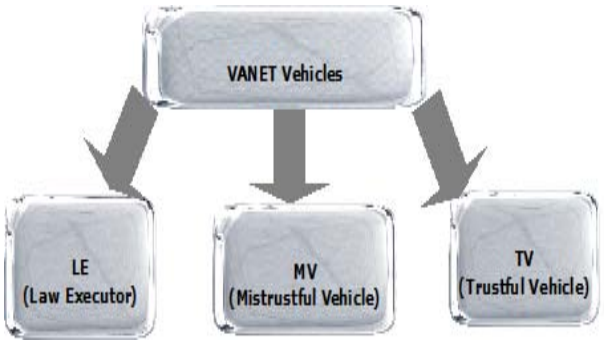

Figure 3. Vehicles Classification in VANET.

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

2. RELATED WORK

It has been demonstrated that problem of VANET is vehicle protection from theft, prevention from sudden accidents, unwanted malicious attacks, communication with other vehicle in a secure way. It means, achieving secure communication among nodes is must to prevent such attacks. So, many schemes emerged to achieve secure communication among nodes. Raya and Hubaux [1] preloaded each vehicle with a large number of anonymous public and private key pairs. However, this approach works good but with high computation cost, high storage space, and high communication overhead. And also, this scheme is not suitable for highly dynamic environments like VANETs. 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 which results in low storage space. However, this method also leads to a high computation cost. Gowtham [17] achieved communication between nodes take place in secured way by using security algorithms similar to ECDSA and TESLA. VANET uses a hardware known as TPD to provide security to nodes [20] in communication process. For sample example please refer [22] Jae Chang and Mark Claypool explained example. To achieve fast communication with security is one of the major problems in VANET. So, in order to achieve fast and secure communication many schemes emerged by using many methodologies. From these, ECC [23] method by Menezes, S. Vnstone, and D. Hankerson achieved best security but with high computation cost. So, in order to overcome this disadvantage, Sirwan A Mohammad and Dr. Sattar [24] developed wireless network based on ns2. But, unfortunately, this scheme also leads to high storage space and also to achieve general authentication in this scheme, requires many steps. From these all schemes, a scheme proposed by Zhang [7] which uses symmetric key hash function and Trust Extended Authentication Mechanism by Ming-Chin Chuang and J.-F. Lee [25] by using XOR operation are best schemes. But, these schemes lead to long authentication latency.So, in order to overcome this drawback, we proposed a scheme called Gamma Protocol Using Modular Arithmetic techniques.

3.PROBLEM STATEMENT

Security is major problem in VANET because it can be easily attacked by attackers. Therefore, there is a need for efficient and robust authentication scheme. So, in order to achieve better authentication for VANET many schemes emerged. But all of these schemes have some problems**.**In all these base schemes, main problem was all responsibility goes to LE. If LE is malicious node then calculations of network groups are going to be wrong, mainly storage space,computation costcalculationsare very high. Hashing method introduced in VANET works in excellent manner, but its keys are easily attacked. Hence, there is a need for an efficient, robust and secure authentication scheme for VANETs with low computation cost, low storage space and short authentication latency. So, in order to give fast and reliable security, we provide Gamma Protocol which uses RSUs-based and on modular arithmetic techniques.

4. PROPOSED WORK

Number theory plays an important role in cryptography. Modular-arithmetic-based concept is the central mathematical concept in number theory. Modular arithmetic approach was developed by **Carl Friedrich Gauss.** "Modulus" (abbreviated as "mod") is the word for "residue or remainder". The difference between normal arithmetic and modular arithmetic is that modular arithmetic operations are performed regarding a positive integer where numbers "wrap around" upon reaching a certain value i.e. "mod". In

VANET, asymmetric key is better than symmetric key if only there will be fast communication and short communication latency.Best examples to public key cryptography algorithms are RSA and DHA. In modular arithmetic operations, multiplication operation i.e. mod multiplication is much more secure. So, in asymmetric key, we use modular arithmetic techniques very much. Gamma Protocol also uses asymmetric key and mod multiplication operation. Consider two nodes under same network under one topology want to communicate with each other to achieve fast communication , then they select one prime number such that prime number greater than zero. And select one primitive root of that prime number such that, that primitive root is less than the chosen prime number. After they select two secret keys and compute respective public values. Here, they exchange these public values and compute common keys by using modular arithmetic techniques. This step gives moresecurity. If that keys are equal, then vehicles behave like TVs and authenticate nearby vehicle to make turn that vehicle into TV. Thus all vehicle communicate with each other after turning into TV, otherwise they behave as MV i.e. Normal vehicle. Thus whole network will be formed for fast communication.

A. Software Testingand Implementation

A network simulator predicts the behavior of a computer network environment and it gives accurate understanding of system behavior. It is designed specifically for research in computer communication networks [26]. So, we can say the network simulator is the bank of different network and protocol objects [25]. 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 is used for specifying scenarios, traffic patterns and events. We carefully analysis the trace files for calculating the performance of network protocols.

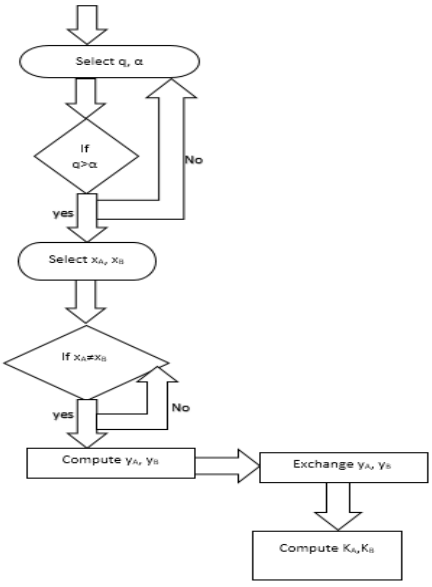

Figure 4. Operations of TV and MV.

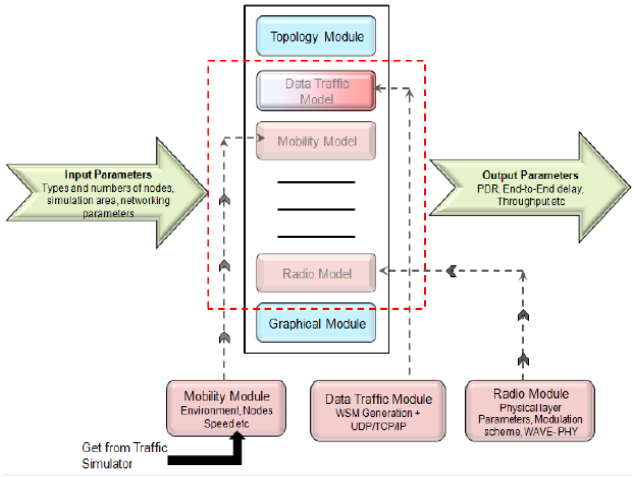

Figure 5.A Typical Design of Network Simulator [18].

NAM [21] is abbreviated for Network AniMator and is visualization tool used 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. Xgraph is X-windows application and analysis tool used for seeing simulation results in the form of graph i.e. to plot the characteristics of NS2 parameters like throughput, End-to-End Delay and packet loss etc...

5. SIMULATION RESULTS

In this section, we analyze the performance of Gamma Protocol and see the simulation results in Xgraph. We used five different source codes, DropTail queuing mechanism and AODV Routing Protocol.

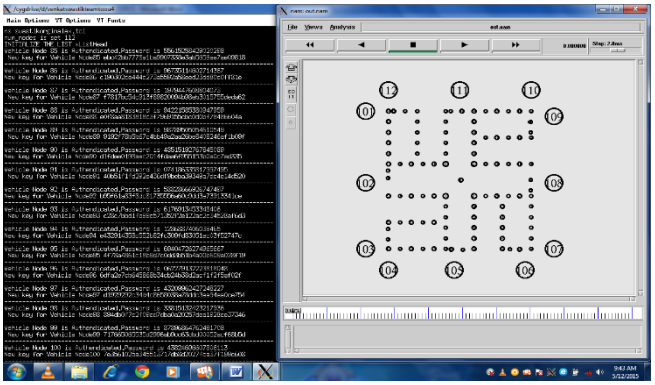

Figure 6. Code Output in NAM.

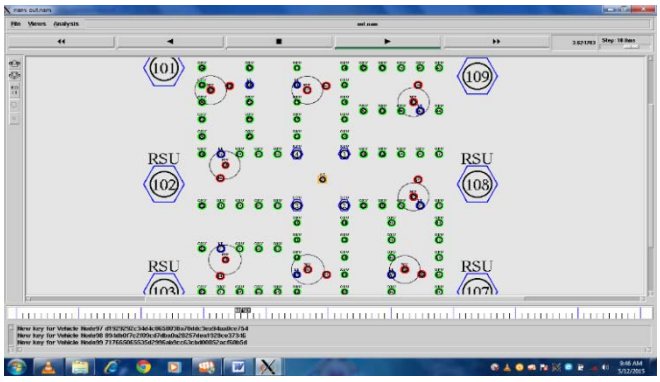

Figure 7. Communication Flow in Network.

Figure 8. Communication betweena LE and a MV.

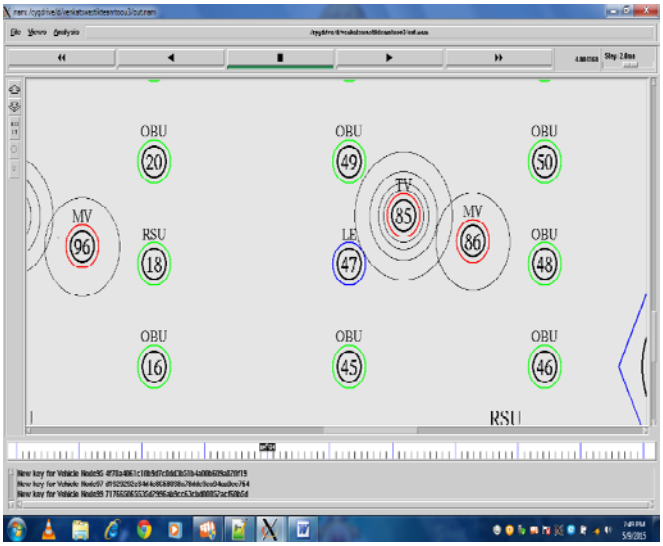

Figure 9.A MV changing into TV.

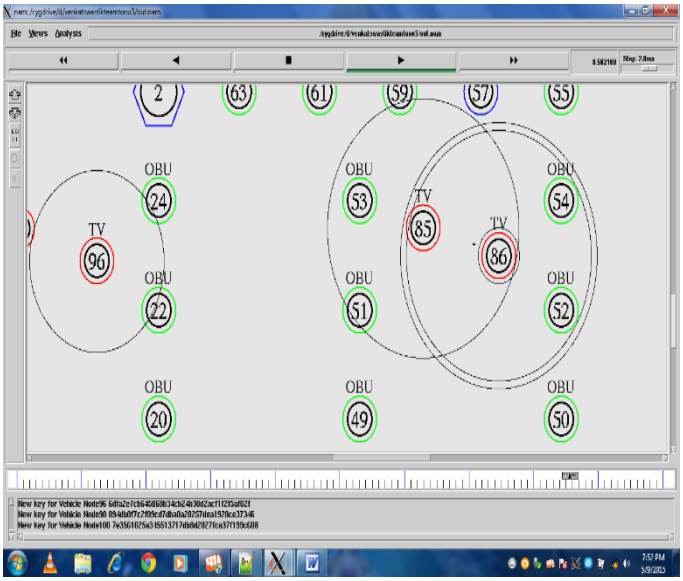

Figure 10. Finally Both MVs Change into TV.

A. Throughput

It is defined as rate of successful message delivery over a channel or aggregate number of packets delivered over the simulation time. Mathematically it can be written as:
Throughput=N/100
Where N is the number of bits bought by all destinations.

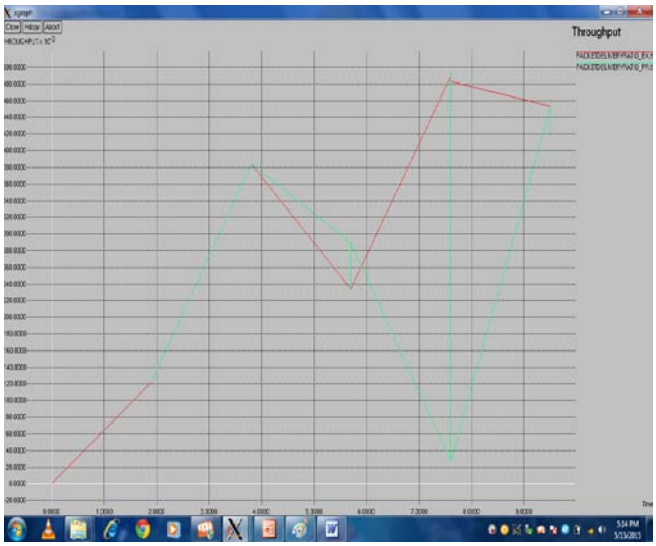

Figure 11. Throughput Graph.

B. End-to-End Delay

It is defined as time taken for a packet to be transmitted successfully across a network from source to destination. Mathematically it is defined as:

$$AED = \frac{\sum_{i=0}^{n}(t_i(r) - t_i(s))}{n_{pr}}$$

Where AED is average end to end delay $t_i(r)$ is the receiving time of packet I by the destination node, $t_i(s)$ is the sending time of packet i by the source node and $n_{pr}$is the total number of packets received.

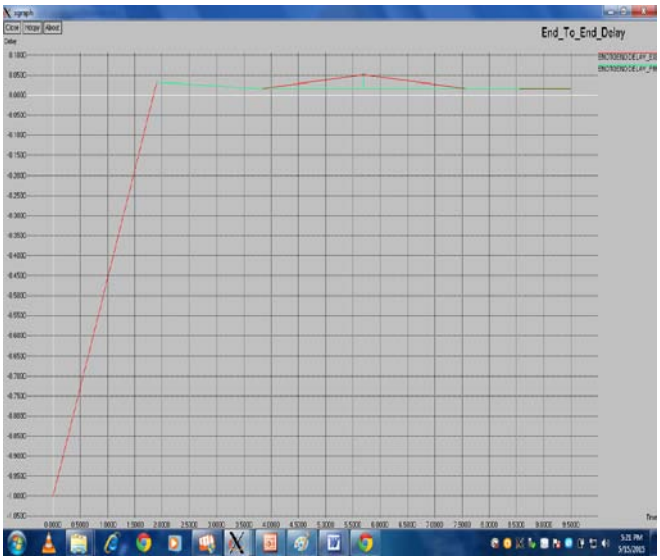

Figure 12. End to End Delay Graph.

C**. Packet Loss**

It is defined as number of failed packets to reach destination from source during transmission. Packet loss occurs due to network congestion. Mathematically it can be calculated as:

Packet Loss=$\frac{N}{S}$

Where N is packet lost and s is the packet sent.

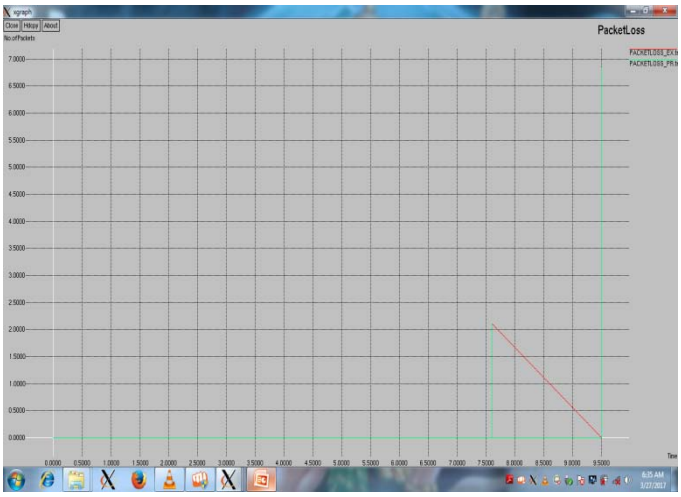

Figure 13. Packet Loss Graph.

From the results obtained, it is concluded that Gamma Protocol is better than base methods which are existed before this protocol.

6. CONCLUSION

Fast communication and security are the major achievements for implementing the VANET. In this paper, we study the proposed scheme called Gamma Protocol to protect valid users in VANET and fast communication requirements. Confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data. The amount of cryptographic calculation under proposed scheme was substantially less than in existing schemes. Moreover, Gamma Protocol is based on the concept of transitive trust relationships to improve the performance of the authentication procedure. In addition, Gamma Protocol has a few storage space to store the authentication parameters than existing system.

7. 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 areDr. S. Anathimadam 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.)Dr.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 toProf. (ret.) Ramana Murthy M. V., Department of Mathematics & Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, and Prof. (ret.) Shankar B., Department of Mathematics, University College of Science, Osmania University, Hyderabad, Telangana and Radhakrishna Peddiraju 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 muchDept. of NS &IT Scholars!

8. 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] 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.

[3] Maxim Raya et al., “The Security of Vehicular Ad Hoc Networks,” SASN’05, Nov 7 20005, Alaxandria, Verginia, USA, pp. 11-21.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

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

[12] 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.

[13] Kevin Fall, Kannan Vardhan, “The ns manual,” The VINT project, December 2008.

[14] Brent Welch, “Practical programming in TCL and Tk,” Prentice Hall, May 1994.

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

[16] www.roadtraffic-technology.com

[17] 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.

[18] www.researchgate.net

[19] 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).

[20] 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.

[21] http://www.isi.edu/nanam/ns/tutorial/index.html

[22] http://www.nile.wpi.edu/ns

[23] Menezes, S. Vnstone, and D. Hankerson, "Guide to elliptic curve cryptography," Spinger Professional Computing (Springer, New York 2004)

[24] 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)

[25] http://iitkgp.vlab.co.in/?sub=38&brch=121&sim=561&cnt=1

[26] http://www.tutorialsweb.com/ns2/NS2-1.html

Authors Biographies

Dr. S. Ananthi (ananthipradeep84@gmail.com)

got her B.E. in Elec. & Commn. Engg. from College of Engineering, Anna University. She did M.Tech. at the Indian Institute of Science (IISc), Bangalore and later did Doctorate from the Instrumentation Centre of Madras University. Presently she is working as Associate Professor and Head i/c, Dept. of Network Systems and Information Technology, University of Madras. Her areas of specialization are in Electrical & Electronic Instrumentation, Microcontrollers, Medical Electronics, Digital Communications, Network Security & IT. She has made extensive contributions and written many books in the above fields. Has guided several Ph.D. candidates. She is a DST Nominee for Science communication Chapter.

Dr. K. Padmanabhan (ck_padmanabhan@rediffmail.com)

did his Grad.Brit.IRE, B.E. from Guindy Engineering College and Doctorate from the Madras University and has served as Professor and Head of the Instrumentation Centre, University of Madras. After retirement, he is A.I.C.T.E. Emeritus Professor in the Anna University. He is a Fellow of IETE, Senior Member IEEE and Fellow IEE. His areas of specialization range from Applied Electronics, Microprocessors, Instrumentation, Telecommns. And Digital Signal processing. His current interest is on the development of novel DSP based Telecom applications.

Dr.Raghavendra Sharma(drmrsstatou@gmail.com) got his Ph.D. from Telangana State, India and currently he is an Assistant ProfessorandHead of the Department, Department of Statistics at University College of Science,Saifabad, Osmania University, Hyderabad, Telangana, India. He is the author of several papers. He is supervisingd many Ph. D.'s. He has excellent teaching track record.

Dr. K. R. Balaji (balajicisl@yahoo.com)has completed M.sc, M.Phil., Ph.D. currently he is working at University of Madras,Guindy Campus, Chennai,Tamil Nadu, India in the department of network systems & information technology, Guindy Campus. He is the author of several papers. He has presented papers at the National and Interactional conferences relating to convolutional encoding and fuzzy based decoding as alternative to Viterbi's decoder. His special interests are in Telecommunication Engineering and Mobile wireless sensor networks

Arun Ananthanarayanan (aarun_84@yahoo.co.in) has finished his M.S from University of buffalo, New York, America. Currently he is pursuing Ph. D. from Univerity of Madras, Department of NS & IT, Guindy campus, **Chennai,** Tamil Nadu, India. He is expert in Image Processing and Speech Recognition.

Rama J (ananthipradeep84@gmail.com), Doctoral Scholar in University of Madras,Guindy Campus, Chennai,Tamil Nadu, India in the department of network systems & information technology, Guindy Campus. Her Research work focuses on modern electonics like VLSI.

Mr.VenkatamangaraoNampally(n.venkat018@gmail.com)

pursed Bachelor of Science in Computer Science, Master of Science in Computer Science and Master of Technology in Computer Science & Engineering from Osmania University, Hyderabad, Telangana, India and pursed Master of Philosophy from University of madras, Chennai, Tamil Nadu, India. He is currently persuing Ph.D. in Computer Science from Osmania University, Hyderabad, and Telangana, India. His main research work focuses on Cryptography Algorithms, Network Security, and Privacy. He has 7 years of teaching experience and 2 year of Research Experience.

