iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4012

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Novel Work for Improving Security and Challenges using Fuzzy Logic Approach in VANETS

B. Gopinath[1], B. Purushothaman[2]
[1]*Dept of ECE, Sona College of technology-Salem, Anna University, Tamilnadu, India.*
[2]*Dept of CSE, Adhiyaaman College of engineering-Hosur, Anna University, Tamilnadu, India.*

Abstract-Vehicular AdHoc networks are the most emerging technologies in now-a-days. VANETs have many challenges like security and time latency when users are travelling in the roadways. There are many techniques available to overcome this kind of problems. One of the efficient methods is Prediction Based Authentication (PBA), in this scheme vehicle users must generate keys using symmetric cryptography for transmitting the information from one vehicle to another vehicle, Sometimes the generated keys are mismatched or hacked by the users due to key replication. In symmetric cryptography the sender and receiver share the common key for data transmission the security of the network and data are not protected. It will lead to malicious attack, resource cannot be efficiently used, and authentication based on signature will be mismatch. In order to achieve authentication, integrity and improve the validity of the network we proposed a localization algorithm based on fuzzy set. In this approach we use binary values that lie in the range between 0 to1. Due to this location of the vehicles can be traced easily by dividing the location into zones using localization algorithm. Fuzzy set using two parameters of vehicles namely speed and distance by using best hops node selection from the current forwarding node. The requirements of security like authentication of messages, privacy and tracing of location can be improved.
Key words: VANETs, OBU (On Board Unit), Fuzzy set, Localization algorithm, RSU (Road side Unit)

I. INTRODUCTION

The application of VANETs in wireless communication using variety of techniques that allows vehicles to communicate with one another using road side available infrastructure to improve the road safety and driving skills such a network is Vehicular AdHoc Networks. VANETS helps to broadcast the vehicles information like speed, distance, status of driving, traffic jam using multihop routing. The value added services like traffic and flow control can be recorded in black block it helps to overcome the traffic functionalities to avoid and reconstruct the scenarios of accidents. RSU can be used to transfer the information to vehicle users within the network, combination of multiple OBUs are called Road Side Unit. In existing methods we should generate keys and they are used for communicating the packets. These results are not accurate due to the duplication of keys and the number of collide packets should be high. In this proposed approach the binary values are used as an input and user need not to generate keys .The solutions should be accurate and it avoids time delay. The system action depends on state of the roadway and traffic in that region. The vehicle status can be monitored by GPS (Global Positioning System). The mobility of the vehicles depends upon streets on road. By using fuzzy set we get best results.

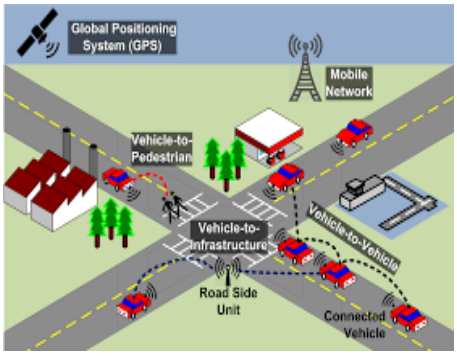


Fig.1.Vanet Communication

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. EXISTING METHODOLOGY

In existing VANET system the number of vehicles arrived in the network should be maximum at short time period. At this situation the location of the vehicles can be identified by signature verification and prediction based authentication scheme. Due to this process the packet collision should be high and time delay also increased. So the successful packet transmission goes to minimum range. The keys can be easily replicated. All the vehicles must predict their location at every time interval. The computational cost should be high. The keys must be generating for each beacon interval for data transmission. So the system has less memory and it is the easiest way to wrong key allocation. Due to this wrong key allocation the data packet will be collide.

III. PROPOSED METHODOLOGY

In this proposed approach fuzzy set can be used. Fuzzy system value lies between 0 and 1.It helps to overcome the drawbacks in existing method the initial step is to grouping the vehicles based on their regions. The central node co-ordinate all the vehicles in their region. Then choose the adversary node it can be used for relaying the node information. At the final step the localization algorithm helps to map the vehicle position in a region. It is also used to monitor the distance between the neighboring vehicles and their speed at the time of data transmission. The above two process are achieved by position metric and distance metric schemes. Finally find the available shortest path to reach the destination then choose the optimal path among these all shortest paths.

A. Grouping of Vehicles

It is the foremost step of proposed approach. All the vehicles in the network are first grouped or clumped. This process helps to all the vehicles to predict their location in the network easily and also helpful to vehicles does not have the capability of communication and which one does not in their region then try to set in their region.

B. Clone Node and Adversary Node Formation

If the vehicle does not have access in spitted region it can be easily detect by adversary node and also include that specific node in data communication. This adversary node have unique checker ID and other nodes are identify with the help of adversary node by its checker ID. This adversary node can be also called as intermediate node. In this process the central network creates clone node. This clone node helps to avoid data loss during data transmission. Due to this clone node formation the source send the messages without any interruptions.

C. Localization Algorithm in Online and Offline Phase

At the final step the localization algorithm can be included. Here we use XED and EDD algorithm. It will be operate in both online and off line mode. So the network can be easily operated. In online phase all the nodes are encountered each other. At online phase each vehicles share their information with other vehicles and the location also updated and even in offline they can communicate to other vehicles when they are not in appropriate position. It helps to avoid the critical situations.

IV. SIMULATION SETUP AND RESULT DISCUSSION

A. Active Queue Management

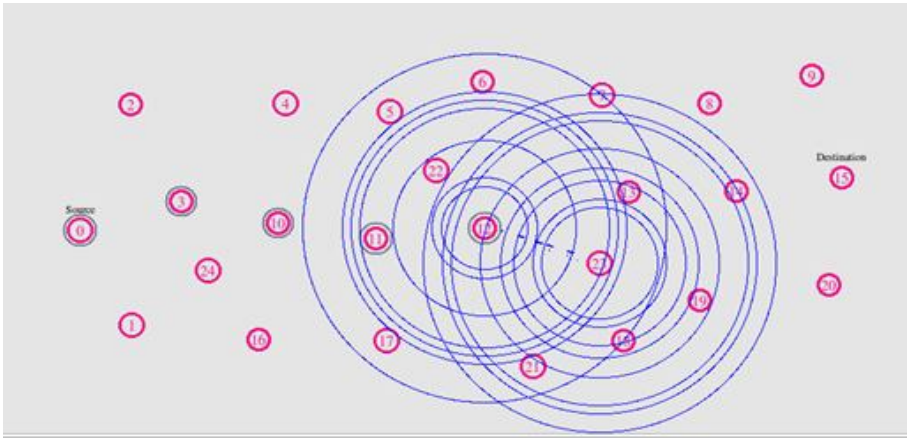


Fig.2 grouping of vehicles

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Adversary Node Formation

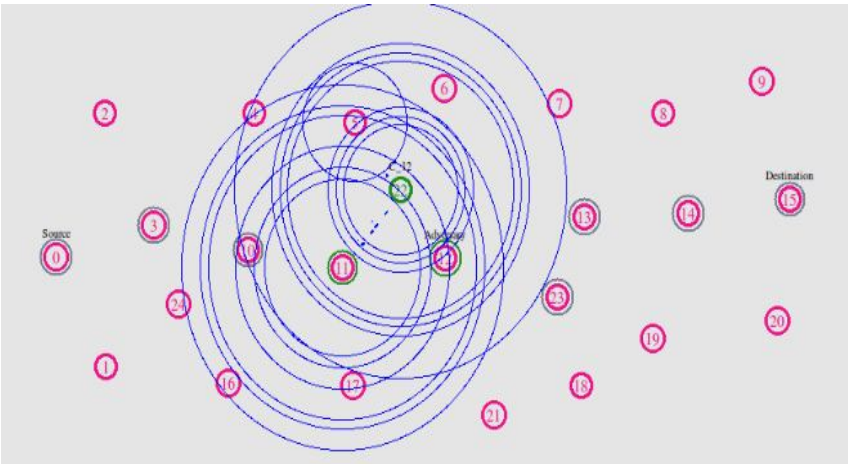


Fig.3 Adversary node Formation

C. Information Gathered by Adversary Node

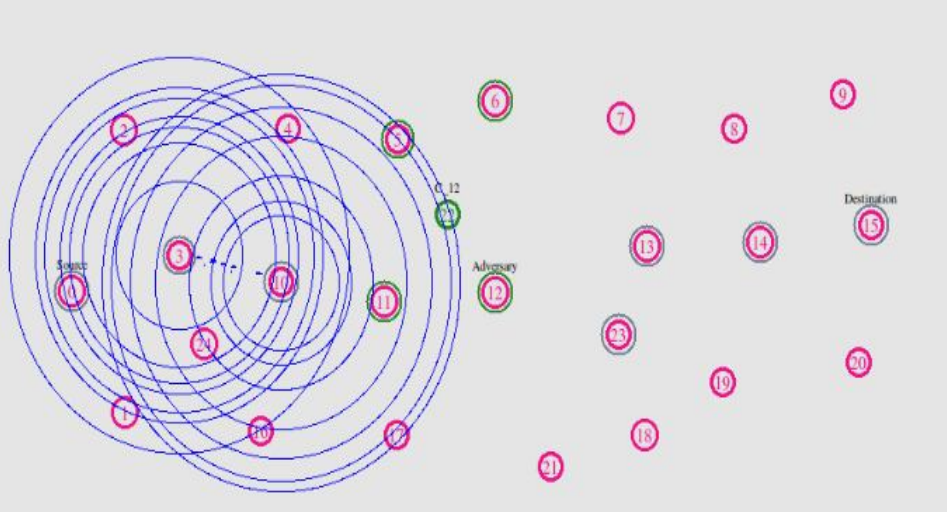


Fig.4 Action of adversary node

D. Data Loss

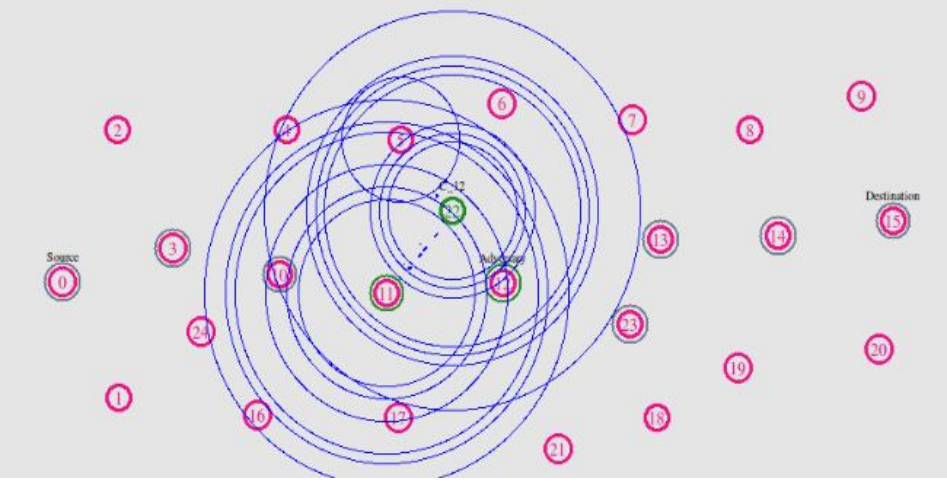


Fig.5 Data loss

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

E. Data Transmission

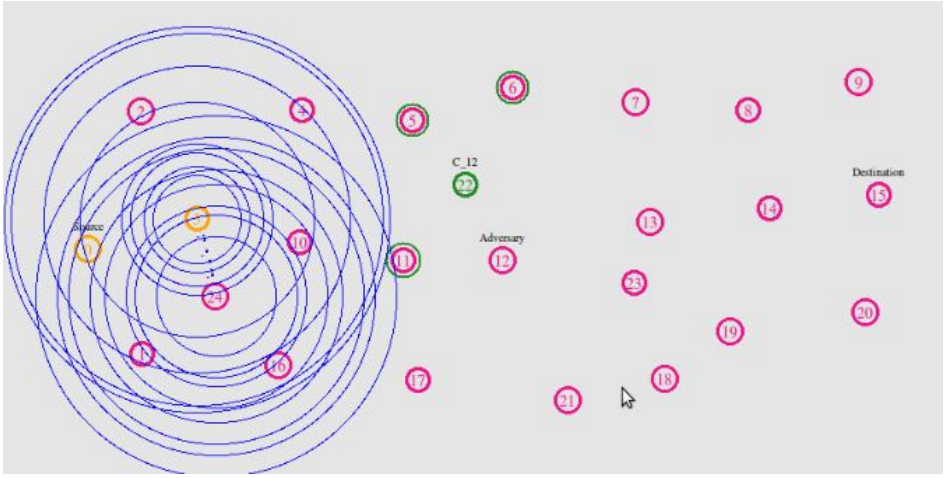


Fig.6 Data Transmission

F. Optimal Path

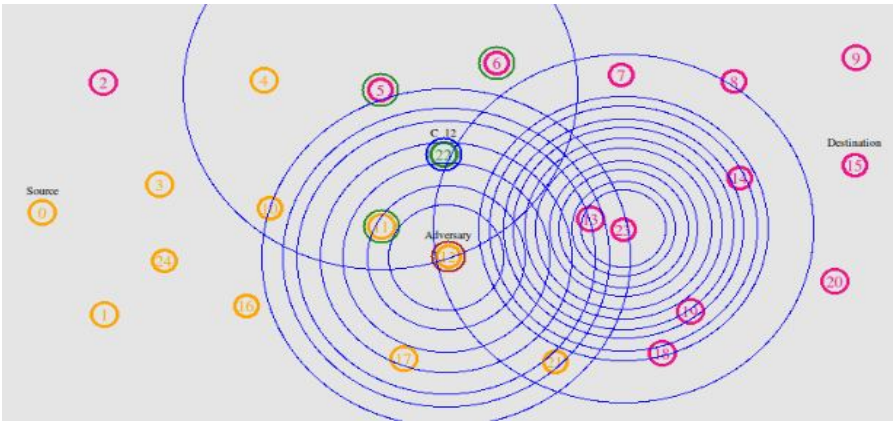


Fig.7 Optimal Path

G. Throughput

Fig.8 Throughput

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

H. Network Coverage Area

Fig.9 Network Coverage Area

I. Packet Loss

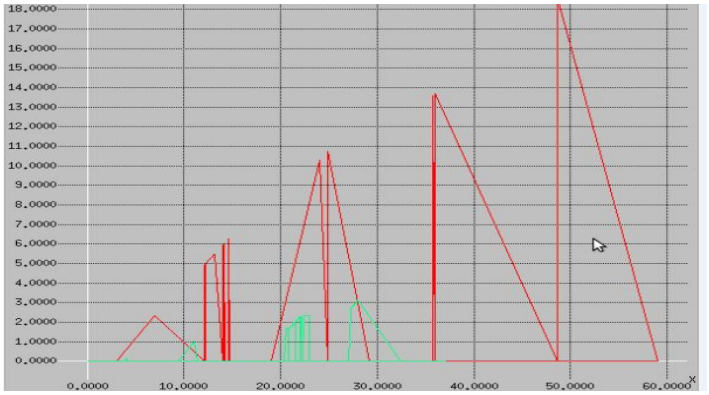


Fig.10.Packet Loss

V. CONCLUSION

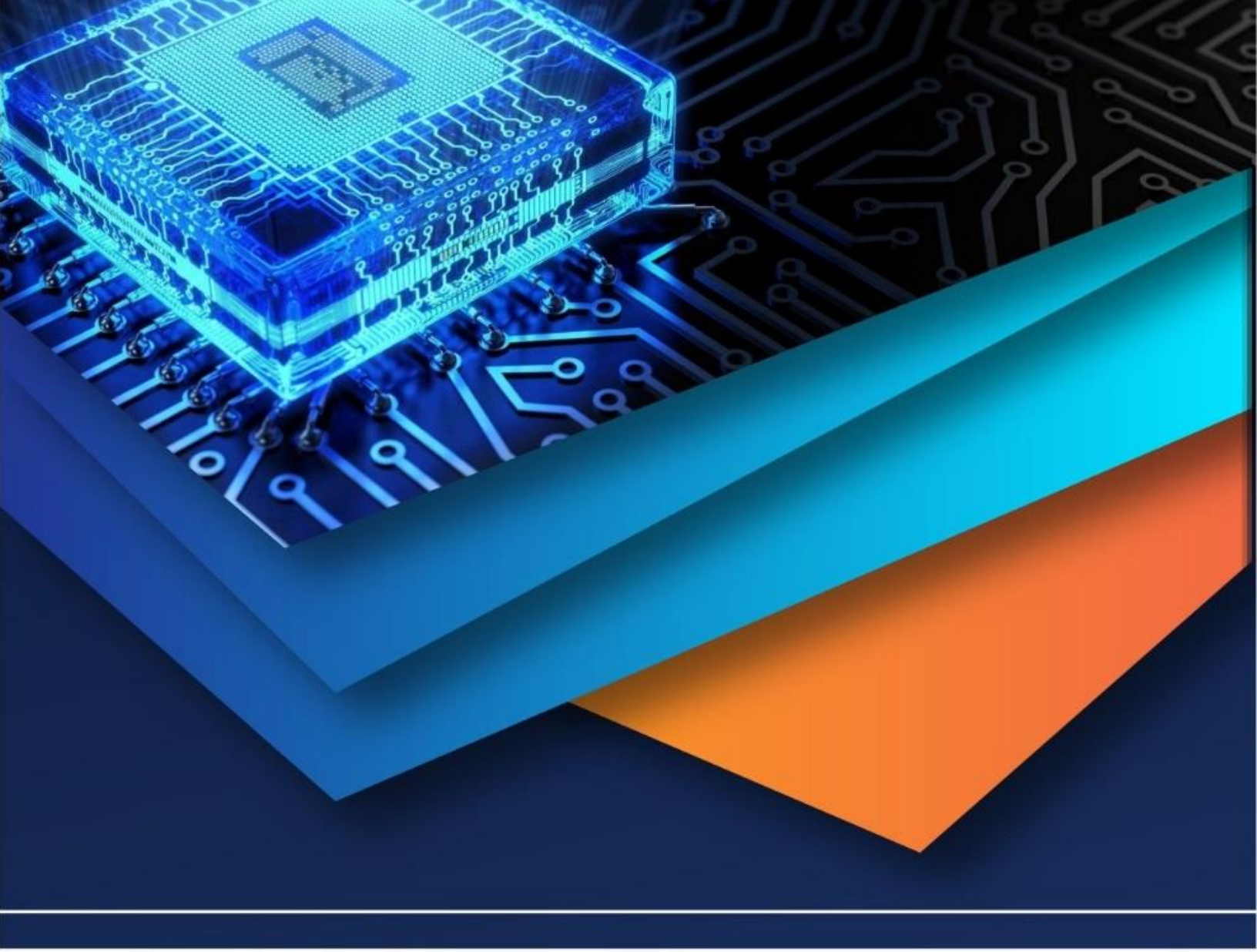
By this fuzzy approach we can avoid traffic jams and accidents. The network coverage area has been increased compared to other existing methods. The successful packet delivery ration that means throughput will be improved. Finally the amount of collide packet should be approximately 15-10% reduced. The system will be easy to implement and users can get accurate results due to implementing the fuzzy set value.

REFERENCES

[1] P.Sheela Rani and R.Vinston Raja "Implementing Efficient Prediction Based Algorithm for Vehicular AdHoc Networks" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 2, February 2015.
[2] N. Lyamin, A. Vinel, M. Johnson, and J. Loo," Real-time detection of denial-of-service attacks in IEEE802.11p vehicular networks," IEEE Communication Letters, vol. 18, no. 1, pp. 110-113, Jan. 2014.
[3] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in Proceedings of IEEE Symposium on Security and Privacy, pp. 174-188, 2013.
[4] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular AdHoc networks, " IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262,Jan. 2011.
[5] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proceedings of the Fourth Workshop Hot Topics in Networks (Hot Nets-IV), Nov.2005.
[6] S. John Moses and P. Anitha Christy Angelina" Enhancing the Privacy through Pseudonymous Authentication and Conditional Communication in Vanets "International Journal of Engineering and Science, Vol. 2, pp. 45- 49, mar 2013.
[7] Rasika Nerkar and Jag dish Pimple "A Survey on Efficient and Secure data transmission for MANET," International Journal of Computer Science and Information Technologies, Vol. 6 (4), 2015, 3709-3711.
[8] Xiang Li, Na Ruan, Fan Wu, Jie Li and Mengyuan Li "Efficient and Enhanced Broadcast Authentication Protocols based on Multilevel μTESLA," IEEE 978-1-4799-7575-2014.
[9] A. Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," IEEE Transactions on Mobile Computing, vol. 12,no. 1, pp. 78-89, Jan. 2013.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653

[10] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM, pp.816–824, 2008.
[11] Time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," IEEE Commun. Lett., vol. 18, no. 1, pp. 110–113,Jan.2014.
[12] N. Lyamin, A. Vinel, M. Johnson, and J. Loo,"Real-Time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," IEEE Commun. Lett., vol. 18, no. 1, pp. 110–113, Jan. 2014.
[13] PBA: "Prediction-Based Authentication for Vehicle-to-Vehicle Communications" Chen Lyu, Dawu Gu, Yunze Zeng and Prasant Mohapatra IEEE transactions on dependable and secure computing vol. 13, no. 1, Jan / Feb. 2016
[14] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proc.Fourth Workshop Hot Topics Network., Nov. 2005.
[15] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Computer Secure. vol.15, no. 1, pp. 39–68, 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY