ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

A Privacy-Preserving Authentication Scheme Based on Hybrid Cryptography for VANET

Manisha Patoniya [1], Prof. Ankit Tripathi [2]

M.Tech Scholar, Department of Electronics and Communication, SCOPE College of Engineering, Bhopal, India[1]

Assistant Professor, Department of Electronics and Communication, SCOPE College of Engineering, Bhopal, India[2]

ABSTRACT: Throughout the years, territory of Vehicular Specially appointed Network accomplished immense intrigue and research activities are additionally expanded because of the scope of arrangements it can give. Data wellbeing is considered as most basic issue in any system framework and it additionally the case in VANET. In VANETs remote discussion between autos along these lines assailants break secrecy, security, and validness properties which sway further assurance. This paper shows the security challenges and existing strings in the VANET framework This paper actualizing hybrid encryption methods i.e AES and RSA calculation and examination their execution. MATLAB software is used to implement algorithm and check the communication authenticity. Simulation time, Buffer size, throughput etc parameters are calculated.

KEYWORDS: VANET, WI-FI, Node, Hybrid, MAC, RSU.

I. INTRODUCTION

Security a Vehicular Specially appointed System, or VANET, is a type of versatile impromptu system, to give interchanges among close-by vehicles and among vehicles and closest fixed hardware, typically portrayed as roadside gear. The VANET used to giving wellbeing and solace to traveler. Having VANET inside vehicle need just little electronic gadget, which will give Impromptu System network to the travelers inside the vehicle. By this gadget working this system does not require confounded association and server correspondence. Every vehicle outfitted with VANET gadget will be a hub in the specially appointed system and can get and hand-off others messages through the remote system In vehicular Specially appointed system utilizing distinctive impromptu systems administration advances, for example, WiFi IEEE 802.11 b/g, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for simple, exact, powerful and basic correspondence between vehicles on unique versatility.

All in all, convention design accomplishes for correspondence among system hubs and gives the structure to execution. When structuring the correspondence suit for VANETs two methodologies can be taken: First, after the customary methodology, the general usefulness could be de-made and sorted out in layers with the end goal that at the conventions satisfy little, all around characterized assignments and structure a convention stack as in TCP/IP and OSI. Second, one could endeavor to construct an altered arrangement that meets the necessities of VANETs with such non-layered.

The primary methodology—called layered methodology and delineated endeavours to hold the request of capacities and convention layers with very much characterized interfaces between them. It adjusts framework functionalities to the requirements of a VANET correspondence framework coming about, e.g., in convention layers for single-jump and multi-bounce correspondence. The restrictions and rigidity of conventional system stacks when utilized in impromptu systems are outstanding. E.g., each layer is actualized as a free module with interfaces (SAPs) just to the abovementioned and underneath layers. Thusly, conventions cannot actually get to state or metadata of a convention on an alternate layer what makes information collection troublesome. Also, some of VANET-explicit capacities don't fit into the customary layered OSI demonstrate, for example, those for system strength and control, and can't be exceptionally doled out to a specific layer. It is likewise important that each layer gets to outside data independently with no basic interface which may prompt issues when this data impacts convention stream.

The second un-layered methodology would be the consequence of fitting an entirely different framework to the necessities of VANETs' fundamental center, i.e., wellbeing applications. Having exact details of these applications and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

willing to utilize the 'probabilistic' divert in the most effective way prompts have a very coupled arrangement of conventions. In this way, all application and correspondence conventions are set in one single coherent square directly over the physical interface and associated with the outside sensors. Inside this square, all convention components are modularized with the end goal that there are no limitations for collaboration, state data is subjective open. Note however, that this 'engineering' acquires a high plan multifaceted nature because of discretionary and complex connections of their modules. This makes convention particular a convoluted work thus, when planned turns into an amazingly unbendable framework for different kinds of use. Additionally it is hard to methodically maintain a strategic distance from control circle, what is fairly simple in the layered methodology with its tidy best down or base up parcel traversal while the two methodologies would surely be plausible.

Human lives in the road are the genuine concern nowadays, in light of the manner in which those reliably endless get-togethers passed on in road mishaps over the world. Vehicular Off the cuff framework (VANET) is phenomenal kind of framework that intends to lessen passing rate and updates improvement achievement structure, where centres clue vehicles.

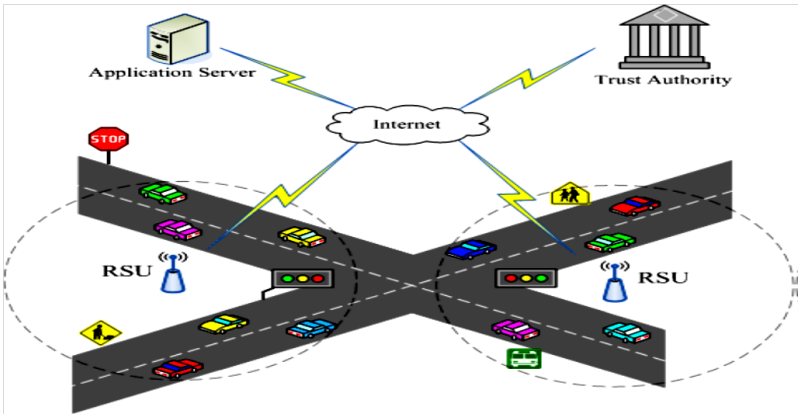


Figure 1: Architecture of VANET

The essential objective of VANET is to give street flourishing evaluations where data about vehicle's present speed, zone empowers are passed with or without the relationship of Establishment. Next to thriving measures, VANET in like way offers some favorable position included associations like email, sound/video sharing, and so on.

II. RELATED WORK

S. Tangade et al., [1] present scheme employs a hybrid cryptography. In DSPA, the asymmetric Identity-Based (ID-based) cryptography and the symmetric hash message authentication code based authentication are adopted during vehicle to infrastructure and vehicle to vehicle communications, respectively. Extensive simulations are conducted to validate the present scheme by comparing the existing works based on PKI, ID-based, group signature, batch verification, and HMAC. The performance analysis showed that DSPA is more efficient, decentralized, scalable, and also a privacy-preserving secured scheme than the existing authentication schemes. Yanbing Liu et al., [2] presents, effective validation arrangements anticipating unapproved guests should be routed to adapt to these issues. Subsequently, in this work it center around the security and protection saving by building up a double verification conspire for IoV as indicated by its diverse situations. In the first place, the OBU self-creates an unknown personality and impermanent encryption key to open a validation session. Second, the authenticity of the vehicle's genuine and mysterious personality can be confirmed by trust specialist.

Slamet indriyanto et al., [3] present the methodology which depends on VoIP over VANETs by methods for recreation. For this errand, an execution assessment of different voice codecs and its effect on nature of administration measurements will be investigated, concentrating on between vehicular voice correspondence. To accomplish great outcomes, it use versatility data got from vehicular traffic generator which depends on the genuine road maps of a urban domain. Consequences of the reenactments are introduced as far as both network level, and client level (Mean Assessment Score) measurements. Oznur Ozkasap et al., [4] present that a Vehicular Ad Hoc Network (VANET) is a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

subclass of mobile ad hoc network, which incorporates smart vehicles and roadside units. It keeps up vehicle to vehicle and vehicle to foundation interchanges. The huge highlights of VANET contain self-association, dispersed networking, and exceedingly powerful topology. SeyhanUcar et al., [5] presents two geographic steering conventions grapple based road and Traffic Mindful Directing and Greedy Perimeter Stateless Routing (GPSR) conventions are assessed on genuine city map. Reproduction of VANETs on genuine guide situations give precise outcomes and furthermore valuable to plan and convey VANETs in genuine world. Genuine portability display is vital on the grounds that it reflects true execution of conventions considered. Examination of execution is conveyed as far as throughput, parcel conveyance proportion, bundle misfortune and normal deferral. Reenactment of conventions is conveyed by changing thickness of hubs. A-STAR indicated better execution on genuine city map over GPSR in light of the fact that A-STAR adopted Road mindfulness technique for steering though GPSR takes a shot at Covetous sending and Directing around the edge strategies. S. Karnani et al., [6] scheme has been presents to which uses the concept of data encryption and compression. In current time the focus has been made specialy on cryptography and data compression. In the next phase it have emphasized on compression cryptosystem. Finally, this technique has been discussed which used the concept of data compression and encryption. In this first data is compressed to reduce the size of the data and increase the data transfer rate. Thereafter compress data is encrypted to provide security and safety.

Modulation Technique	Coded Bit Rate (Mbps)	Coding Rate	Data Rate (Mbps)	Data Bits per OFDM Symbol
BPSK	6	1/2	3	24
BPSK	6	3/4	4.5	36
QPSK	12	1/2	6	48
QPSK	12	3/4	9	72
16-QAM	24	1/2	12	96
16-QAM	24	3/4	18	144
64-QAM	36	2/3	24	192
64-QAM	36	3/4	27	216

Figure 2: Data Rate Options in a DSRC 10 MHz OFDM Channel

The personality based bunch check (IBV) plot has been as of late present to make VANETs progressively secure and productive for commonsense use. In this paper, we call attention to that the current IBV plot has some security dangers. We present an improved plan that can fulfill the security and protection wanted by vehicles. The present IBV conspire gives the provable security in the irregular prophet demonstrate. What's more, the clump confirmation of the present plan needs just a little consistent number of blending and point augmentation calculations, autonomous of the quantity of messages.

III. PROBLEM FORMULATION

The size of authentication messages should be small and the process must consume little time to given enough bandwidth and time for useful communication.

Security is the most important part in data communication system, where more randomization in secret keys increases the security as well as complexity of the cryptography algorithms.

- As a result in recent dates these algorithms are compensating with enormous memory spaces and large execution time on hardware platform.

- Response time for selected encryption method must be minimal.
- Security level must be acceptable considering the key lifetime.

In this work, the communication overhead is reduced by employing a single request-reply message exchange between a vehicle and the RSU for authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

IV. PRESENT WORK

The main contributions of this work can be summarized as follows.

In this work, there has been implemented three encrypt techniques like DES, AES and RSA algorithm and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption process and also its buffer size experimentally.

1) Present a novel approach for users to start their connections in the VANET in a secure way.

2) A new hybrid cryptographic approach has been explained that provides much higher security measures compared to existing ones and analyze the performance of our approach using mathematical and simulation means.

3) A novel mechanism has been present for authentication and data confidentiality in VANETs.

4) In present work a node has been designed i.e., RSU and provide such environment so that it can simulate on MATLAB software.

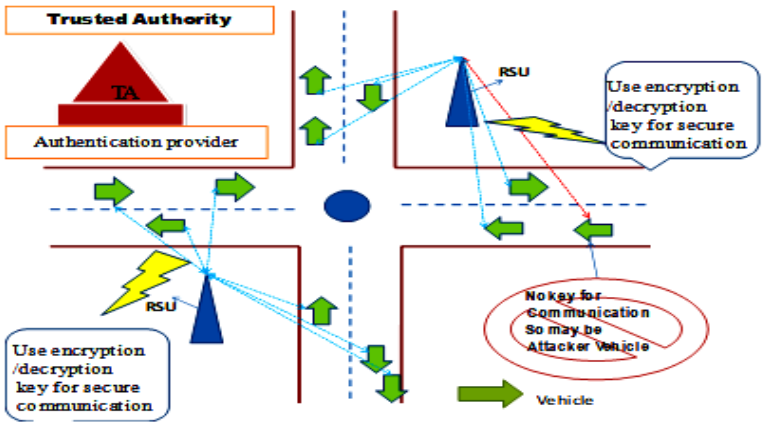


Figure 3: System Model

Figure 3 is showing the system model under consideration. It is consider infrastructure based VANETs in this work, where entities can be classified into three categories: authorities at the root, road side unit, and nodes (vehicles moving on a road)

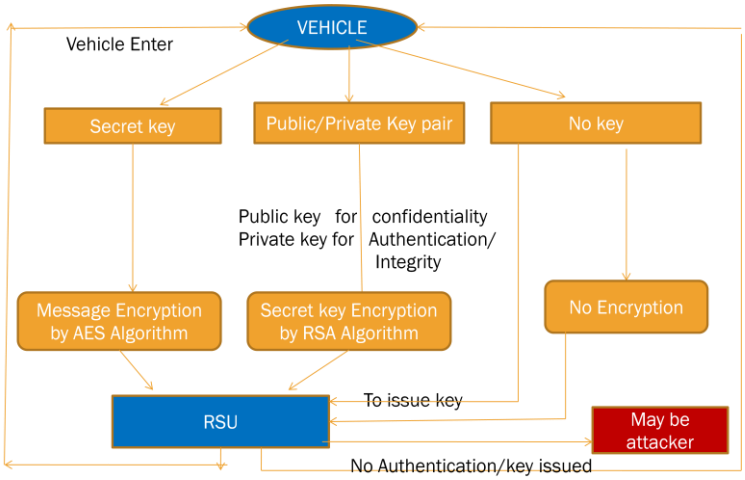


Figure 4: Flow Chart of Present Work

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Protocol Description

An RSU continuously broadcasts its identity RSU_{ID} and public key PB_{RSU} in its area. As a vehicle enters the area of a different RSU, it receives RSU broadcast and determines that needs to associate itself and initiate mutual authentication process. The vehicle encrypts the RSU_{ID} , its V_{ID} and current timestamp t_0 and shared key by the public key PB_{RSU}. This is sent to the RSU. The RSU forwards the encrypted part to the TA. TA authenticates the vehicle and the RSU and sends its authentication details report to the RSU by encrypting the authentication information of the RSU with the vehicle shared key and that of the vehicle to the RSU. RSU confirms the authentication of the vehicle and forwards the encrypted part of the report to vehicle for RSU authentication.

STEP 1: (KEY SETUP)

Key Generation + Authentication:

- Each party generates RSA Public/Private key-pair.
- Each party exchange their public key with each other.
- Vehicle generates 128-bit AES Symmetric Key, encrypts it with public key received from the RSU and sends this encrypted symmetric key to RSU.
- RSU on receiving the encrypted symmetric key, decrypts it with its own Private Key.
- At this stage both parties have the AES 128-bit Symmetric key.

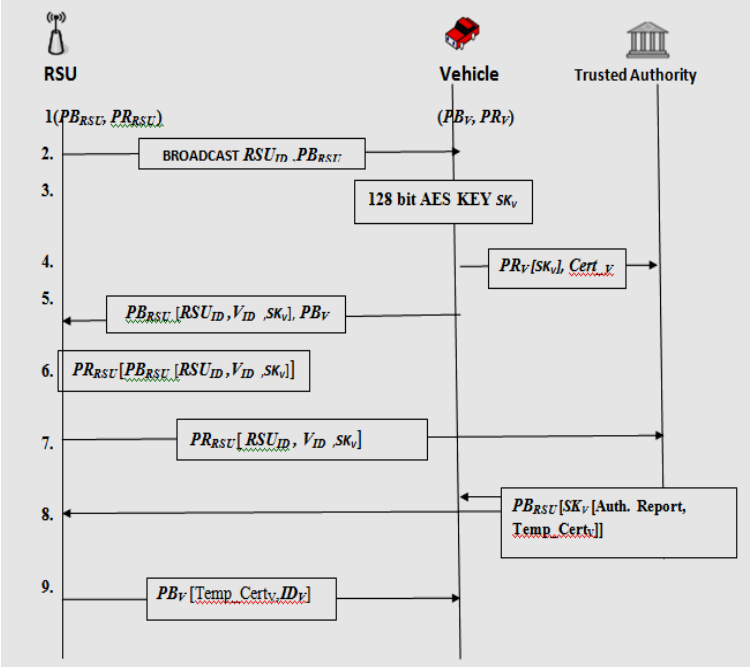


Figure 5: Key Setup for Present Method

STEP 2: Sending a Message (Encryption Process)

- Vehicle wants to send a message to RSU.
- The Message is encrypted with the AES Symmetric Key.
- The Encrypted Message is encrypted with the RSU Public key..
- Then send to RSU.

STEP 3 : Message Received (Decryption Process)

- RSU receives [RSU Public key (AES Symmetric Key)+ (AES Symmetric Key Encrypted Message)].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

- Decryption with gives (RSU Private Key AES Symmetric Key+(AES Symmetric Key Encrypted Message).

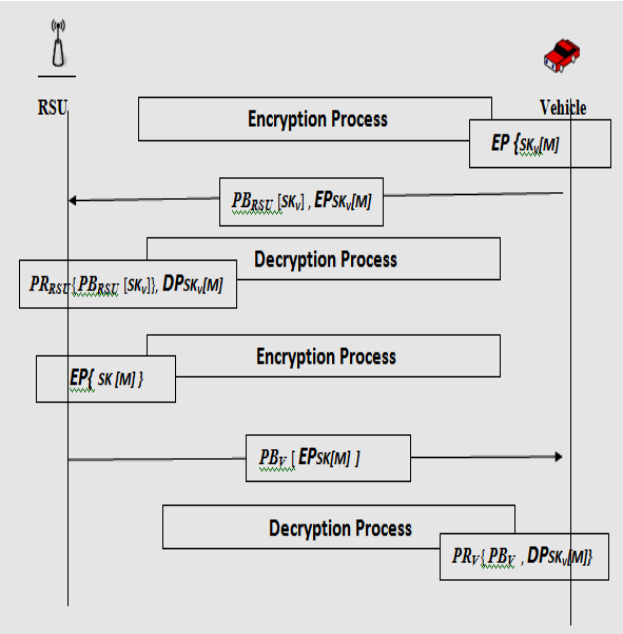


Figure 6: Encryption and Decryption Process for Present Method

V. EXPERIMENTAL ANALYSIS AND RESULT

In this research work following parameters are generating, in which some parameters are improved. The major work of our research is simulation of vehicular network in MATLAB environment. Throughput is also measured in bytes per second, which shows about the performance of different security scheme. Here it can be easily seen based on throughput i.e. hybrid technique is best comparatively others.

$$\text{Encryption Throughput (Byte/Sec)} = \frac{\sum \text{Input Size}}{\sum \text{Encryption Simulation Time}}$$

$$\text{Decryption Throughput (Byte/Sec)} = \frac{\sum \text{Input Size}}{\sum \text{Decryption Simulation Time}}$$

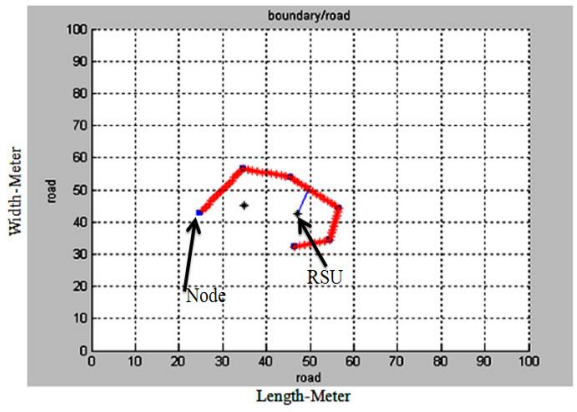


Figure 7: Node with Double RSU

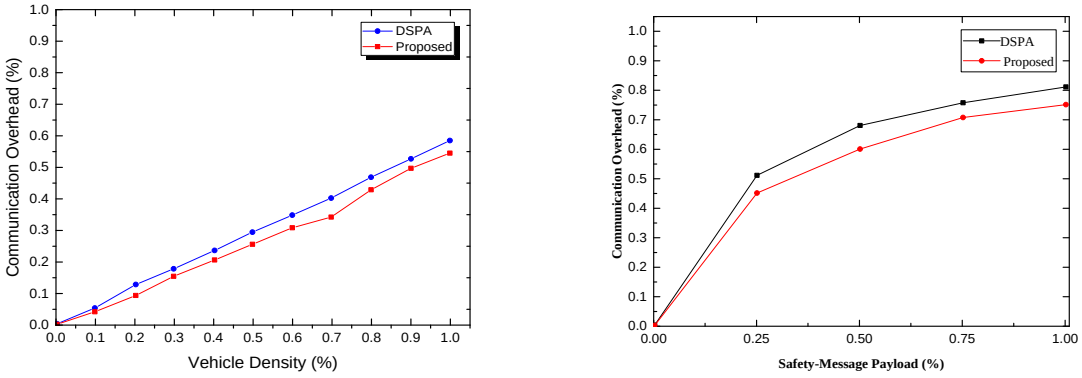
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

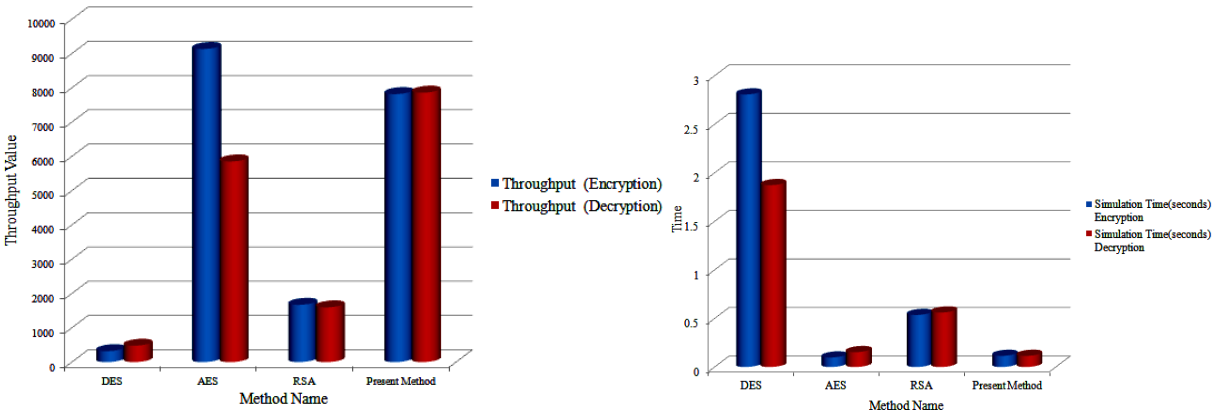
Website: www.ijircce.com

Vol. 8, Issue 3, March 2020



(a) (b)

Figure 8: (a) Communication overhead: Payload = 67 bytes (b) Communication overhead: Payload = 50, 100, 150, and 200 bytes



(a) (b)

Figure 9: (a) Throughput (Encryption and Decryption) (b) Encryption and Decryption time

Table 1: Comparison of present work and previous work

Sr No.	Parameter	Base paper	Present	Improvement
1	Methodology	ID-based + HMAC	RSA+ AES	-
2	Simulation Time (Sec)	200	50	Reduce 4 times
3	Number of RSU	3	2	Reduce 1
4	Number of Vehicles	100	200	2 times Double
5	Packet size (Byte)	256	512	2 times Double

VI. CONCLUSION

Hence, hybrid encryption key-management schemes for a VANET have been performed. From the results it has been shown that there is an increase in the efficiency of the system when there is a present scheme in place of the previous scheme. There is a considerable improvement in the data communication between the nodes after key management techniques have been employed. This technique can be used in security-sensitive applications like police and government agencies where VANETs are increasingly being used. This algorithm presents something that is quiet against the norms prevalent in our times. Almost all public key algorithms coming are based on much more complex

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

mathematical problems as compared to Chinese Remainder Theorem. We believe that to meet stringent efficiency requirements of VANET we will have to look beyond conventional methods and schemes and it certainly does throw light on new areas and possibilities which are there to be explored.

REFERENCES

1. S. Tangade, S. S. Manvi and P. Lorenz, "Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs," in IEEE Transactions on Vehicular Technology, vol. 67, no. 9, pp. 8647-8655, Sept. 2018.
2. Yanbing Liu, Yuhang Wang, and Guanghui Chang" Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm" IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS 2017.
3. Slamet indriyanto1, muhammad najib dwi satria2, andira rizky sulaeman3, rifqy hakimi4, eueung mulyana "performance analysis of vanet simulation on software defined network" may 2017 IEEE
4. Oznur Ozkasap ,Seyhan Ucar, Sinem Coleri Ergen,Individual " Multihop Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination".IEEE transactions on vehicular technology, VOL. 65, no. 4, April 2016
5. SeyhanUcar, Understudy Part, IEEE, SinemColeriErgen, Part, IEEE, and OznurOzkasap, Part, IEEE "Multihop-Group Based IEEE 802.11p and LTE Cross breed Engineering for VANET Wellbeing Message Dispersal" IEEE Exchanges ON VEHICULAR Innovation, VOL. 65, NO. 4, APRIL 2016
6. S. Karnani and M. Singh, "Data Security Through Encryption Technique View More", *SMART MOVES JOURNAL IJOSCIENCE*, vol. 3, no. 5, May 2017. http://ijoscience.com/ojsscience/index.php/ojsscience/article/view/51.
7. Sinem Coleri ,Seyhan Ucar, Ergen, Member, IEEE, and Oznur Ozkasap, Member, IEEE" Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid architecture for vanet safety message dissemination" IEEE transactions on vehicular technology, vol. 65, no. 5, april 2016
8. Megha nema,shalini stalin, " RSA Calculation construct Encryption in light of Secure Wise Activity Framework for VANET utilizing Wi-Fi IEEE 802.11" in IEEE Madhya Pradesh section.10-12sep. 2015.
9. Shalini Stalin, Megha nema, Prof. Vijay Lokhande3, " Investigation of Assaults and Difficulties in VANET" Global Diary of Developing Innovation and Propelled Designing Site: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Guaranteed Diary, Volume 4, Issue 7, July 2014)
10. G. Araniti, C. Campolo, M. Condoluci, A. Iera, A. Molinaro College Mediterranea of Reggio Calabria, Italy "LTE for Vehicular Systems administration: A Survey"IEEE Correspondences Magazine, vol.51, no. 5, pp. 148-157, May 2013
11. khalid abdel hafeez, student member, ieee, lian zhao, senior member, ieee, bobby ma, senior member, ieee, and jon w. mark, life fellow, IEEE "performance analysis and enhancement of the dsrc for vanet's safety applications" IEEE transactions on vehicular technology, vol. 62, no. 7, september 2013 3069
12. Khaleel Mershad and Hassan Artail. "A System for Secure and Productive Information Obtaining in Vehicular Specially appointed "IEEE Exchanges ON VEHICULAR Innovation, VOL. 62, NO. 2, FEBRUARY 2013
13. Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" IEEE transactions on mobile computing, VOL. 12, NO. 1, JANUARY 2013
14. Khaleel Mershad and Hassan Artail "A System for Secure and Proficient Information Obtaining in Vehicular Specially appointed Systems." IEEE Exchanges On Vehicular Innovation, Vol. 62, No. 2, February 2013
15. Shi-Jinn Horng, Shiang-Feng Tzeng, Yi Container, Pingzhi Fan, Senior Part, IEEE, XianWang b-SPECS+: Group Confirmation for Secure VANET" IEEE Exchanges On Data Legal sciences And Security, Vol. 8, No. 11, November 2013
16. Xiaodong Lin, Senior Part, IEEE, and Xu Li "Pseudonymous Confirmation in Accomplishing Effective Helpful Message Validation in Vehicular Specially appointed Systems" IEEE Exchanges On Vehicular Innovation, Vol. 62, No. 2, February 2013
17. E. Coronado and S. Cherkaoui, "Administration disclosure and administration access in remote vehicular systems," in Proc. IEEE GLOBECOM Workshops, 2012, pp. 1– 6.