A Secure Key Algorithm for Sharing Information in Vehicular Ad-hoc Network Systems

[1]Chetan Singh, [2]Shushila Sonare

[1]Research Scholar, [2]Assistant Professor

Department of Computer Science & Engineering,

Lakshmi Narain College of Technology, Bhopal, India

***Abstract* — Throughout the years, territory of Vehicular Specially appointed Network accomplished immense intrigue and research activities is 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 In this paper, actualizing multi 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, Multi, MAC, RSU.

I. INTRODUCTION

Vehicular Uncommonly named Framework, or VANET, is a sort of adaptable off the cuff framework, to give trades among near to vehicles and among vehicles and nearest fixed equipment, ordinarily depicted as side of the road gear.

The VANET used to giving prosperity and comfort to explorer. Having VANET inside vehicle need simply minimal electronic contraption, which will give Off the cuff Framework organization to the voyagers inside the vehicle. By this contraption working this framework doesn't need jumbled affiliation and worker correspondence. Each vehicle equipped with VANET contraption will be a center in the exceptionally designated framework and can get and hand-off others messages through the far off framework

In vehicular Extraordinarily delegated framework using particular improvised frameworks organization propels, for instance, WiFi IEEE 802.11 b/g, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for basic, definite, ground-breaking and fundamental correspondence between vehicles on novel adaptability.

With everything taken into account, show configuration achieves for correspondence among framework center points and gives the structure to execution. While organizing the correspondence suit for VANETs two systems can be taken: First, after the standard technique, the overall convenience could be de-made and figured out in layers with the ultimate objective that at the shows fulfill close to nothing, all around described tasks and structure a show stack as in TCP/IP and OSI. Second, one could try to build a changed course of action that meets the necessities of VANETs with such non-layered.

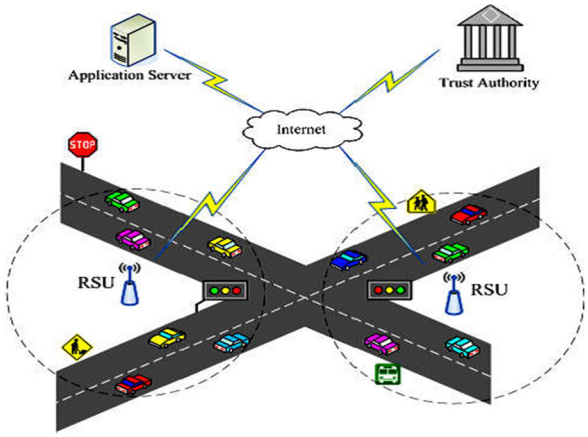


Figure 1: Architecture of VANET

The essential strategy—called layered technique and portrayed in figure 1 undertaking to hold the solicitation of limits and show layers with especially described interfaces between them. It changes structure functionalities to the necessities of a VANET correspondence system occurring, e.g., in show layers for single-hop and multi-ricochet correspondence. The limitations and unbending nature of regular framework stacks when used in unrehearsed frameworks are extraordinary. E.g., each layer is realized as a free

module with interfaces (SAPs) just to the previously mentioned and underneath layers. Consequently, shows can't really will state or metadata of a show on another layer what makes data assortment problematic. Likewise, some of VANET-unequivocal limits don't find a way into the standard layered OSI illustrate, for instance, those for framework quality and control, and can't be especially given out to a particular layer.

The subsequent un-layered system would be the outcome of fitting a totally extraordinary structure to the necessities of VANETs' principal community, i.e., prosperity applications. Having definite subtleties of these applications and ready to use the 'probabilistic' redirect in the best way prompts have a coupled game plan of shows. Along these lines, all application and correspondence shows are set in one single reasonable square legitimately over the actual interface and related with the external sensors (Fig. 2). Inside this square, all show parts are modularized with the ultimate objective that there are no restrictions for coordinated effort, state information is abstract open. Note in any case, that this 'designing' obtains a high arrangement multifaceted nature as a result of optional and complex associations of their modules. This makes show specific a tangled work accordingly, when arranged transforms into an incredibly unbendable structure for various types of utilization. Also it is difficult to efficiently keep up a vital good ways from control circle, what is genuinely straightforward in the layered strategy with its clean best down or base up bundle crossing. While the two procedures would doubtlessly be conceivable human lives in the street is the certified concern these days, considering the way where those dependably unending parties passed on in street incidents over the world. Vehicular Spur of the moment system (VANET) is exceptional sort of structure that plans to diminish passing rate and updates improvement accomplishment structure, where focus focuses hint vehicles.

The fundamental target of VANET is to give road thriving assessments where information about vehicle's current speed, zone enables is passed with or without the relationship of Foundation. Close to flourishing measures, VANET in like way offers some ideal position included affiliations like email, sound/video sharing, etc.

II. METHODOLOGY

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 multi 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.

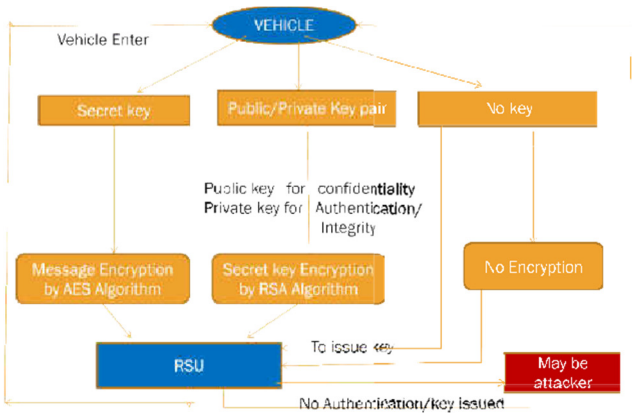


Figure 2: Flow Chart of Present Work

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.

III. SIMULATION 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. multi technique is best comparatively others.

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

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

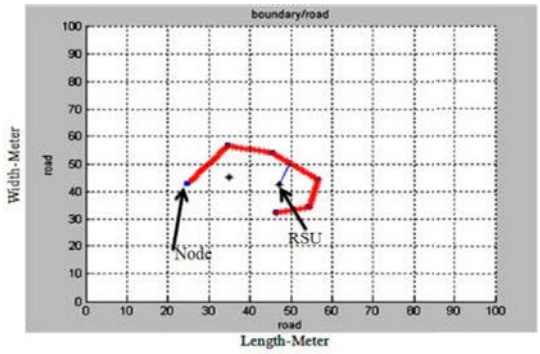
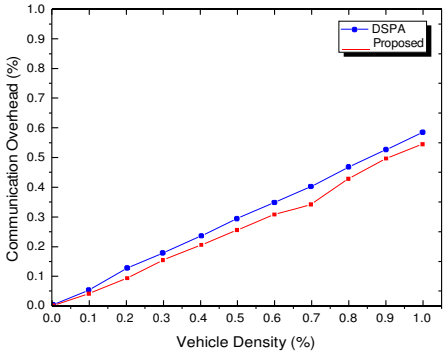
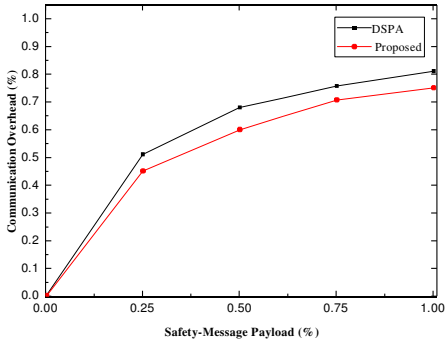


Figure 3: Node with Double RSU



(a)



(b)

Figure 4: (a) Communication overhead: Payload = 67 bytes
(b) Communication overhead: Payload = 50, 100, 150, and 200 bytes

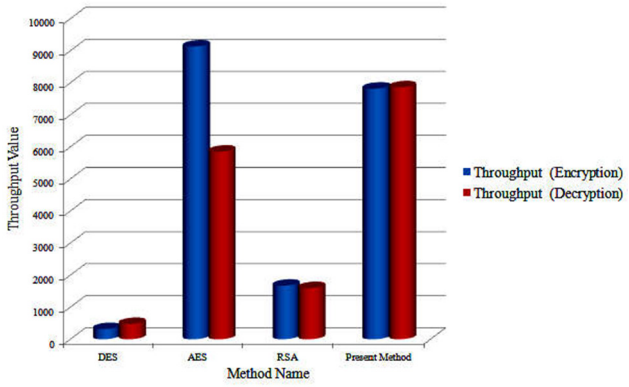


Figure 5: Throughput (Encryption and Decryption)

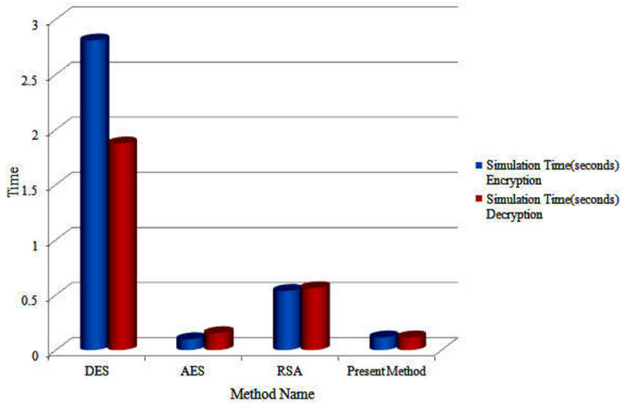


Figure 6: Encryption and Decryption time

Table 1: Simulation Results

Sr No.	Parameter	Present
1	Methodology	RSA+ AES
2	Simulation Time (Sec)	50
3	Number of RSU	2
4	Number of Vehicles	200
5	Packet size (Byte)	512

IV. CONCLUSION

This strategy can be utilized in security-delicate applications like police and government organizations where VANETs are progressively being utilized. This calculation presents something that hushes up against the standards common in our occasions. Practically all open key calculations coming depend on considerably more perplexing numerical issues when contrasted with Chinese Leftover portion Hypothesis. We accept that to meet rigid proficiency prerequisites of VANET we should look past ordinary strategies and plans and it unquestionably illuminates new zones and conceivable outcomes which are there to be investigated.

REFERENCE

1. C. Chen, Y. Chen, C. Lee, Y. Deng and C. Chen, "An Efficient and Secure Key Agreement Protocol for Sharing Emergency Events in VANET Systems," in IEEE Access, vol. 7, pp. 148472-148484, 2019, doi: 10.1109/ACCESS.2019.2946969.
2. S. Kanchan, G. Singh and N. S. Chaudhari, "SAPSC: SignRecrypting authentication protocol using shareable clouds in VANET groups," in IET Intelligent Transport Systems, vol. 13, no. 9, pp. 1447-1460, 9 2019, doi: 10.1049/iet-its.2018.5474.
3. Z. Wei, J. Li, X. Wang and C. Gao, "A Lightweight Privacy-Preserving Protocol for VANETs Based on Secure Outsourcing Computing," in IEEE Access, vol. 7, pp. 62785-62793, 2019, doi: 10.1109/ACCESS.2019.2915794.
4. 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, doi: 10.1109/TVT.2018.2839979.
5. A. Slama, I. Lengliz and A. Belghith, "TCSR: an AIMD Trust-based Protocol for Secure Routing in VANET," 2018 International Conference on Smart Communications and Networking (SmartNets), Yasmine Hammamet, Tunisia, 2018, pp. 1-8, doi: 10.1109/SMARTNETS.2018.8707389.
6. H. Tan, Z. Gui and I. Chung, "A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs," in IEEE Access, vol. 6, pp. 74260-74276, 2018, doi: 10.1109/ACCESS.2018.2883426.
7. D. K. Sandou, N. Jothy and K. Jayanthi, "Secured Routing in VANETs Using Lightweight Authentication and Key Agreement Protocol," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2018, pp. 1-5, doi: 10.1109/WiSPNET.2018.8538678.
2. H. Tan, D. Choi, P. Kim, S. Pan and I. Chung, "Comments on “Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks”," in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2149-2151, July 2018, doi: 10.1109/TITS.2017.2746880.
3. E. R. Agustina and A. R. Hakim, "Secure VANET protocol using hierarchical pseudonyms with blind signature," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-4, doi: 10.1109/TSSA.2017.8272919.
4. K. Lim, K. M. Tuladhar, X. Wang and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 478-483, doi: 10.1109/UEMCON.2017.8249091.
5. S. Chaba, R. Kumar, R. Pant and M. Dave, "Secure and efficient key delivery in VANET using cloud and fog computing," 2017 International Conference on

Computer, Communications and Electronics (Comptelix), Jaipur, 2017, pp. 27-31, doi: 10.1109/COMPTELIX.2017.8003932.

6. L. Wei and C. Zhang, "TrInc-Based Secure and Privacy-Preserving Protocols for Vehicular Ad Hoc Networks," 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, 2016, pp. 1-5, doi: 10.1109/VTCSpring.2016.7504512.
7. P. Vijayakumar, M. Azees, A. Kannan and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 1015-1028, April 2016, doi: 10.1109/TITS.2015.2492981.
8. M. Nema, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375676.
9. J. Zhou, X. Dong, Z. Cao and A. V. Vasilakos, "Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1299-1314, June 2015, doi: 10.1109/TIFS.2015.2407326.