International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Sh-Rsa Messaging Scheme for Secure Communication in Vanet

M.S.Bennet praba, Jack Shelton J, Bhuvanesh k, Ashwin kumar R

ABSTRACT- The term VANET determines the advancements in wireless communications as well as networking automation .The communication between any two vehicles by connecting them through a Wireless Level Area Network (WLAN). This is purely based on Vehicular AdHoc Network [VANET] communication. The objective is to build a Safety-Related application model. In this system, Information can be sent from a vehicle at any kind of emergency time by the user and producing to the other connected vehicle so that the receiver can produce help services to the vehicle. The ID-MAP technique used previously cannot guarantee the level of messaging scheme and the speed of encryption ,decryption gain. We propose a 4 layered theory called "SH-RSA" (Secure-Hybrid-RSA). It is a multi-layered authentication stack which has encryption as well as decryption. Compared to RSA, decryption through SH-RSA has gained 8.53 times than the RSA. Whereas encryption throughput is around 6 KB/SEC.

Index Terms SH-RSA (secure hybrid -Rivest Shamir and Adelman) TTP (Trusted Third Party) CIA (Confidentiality, Integrity and Accessibility) Dedicated Short Range of Communication (DSRC).

I. INTRODUCTION

The term VANET defines the developments in wireless communications and also in the automation of networking and this also increases the efficiency and safety of traffic.

End-to-end security will be the key limitation for LAN-To-LAN tunnels and Virtual Private Networks for private messaging scenarios. End-To-End is a communication system that can only accessed by communicating user, which also excludes Internet providers, providers of telecommunications.

Internet Protocol Security is all about communications, and this causes problems when key is compromised. This resolves with the addition of messaging scheme perfect forward Secrecy. This messaging scheme is the efficient and light-weight for having uniformity with basic requirements. The first public key cryptography systems which is used for transmitting the data for secured way is known as Rivest-Shamir-Adelman (RSA).

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Jack Shelton J, 3rd year student of B.tech CSE from SRM Institute of Science and Technology, Chennai, India.
Ashwin kumar R, 3rd year student of B.tech CSE from SRM Institute of Science and Technology, Chennai, India.
Bhuvanesh K, , 3rd year student of B.tech CSE from SRM Institute of Science and Technology, Chennai, India.
Ms. M.S Bennet Praba*, Assistant Professor, Computer Science Engineering Department in SRM Institute of Science and Technology, Ramapuram, Chennai, India.

It is a popular cipher which is constantly encountered in secure communications which scientifically faces many problems[2].

The advancement of the SH-RSA produces with the greater speed in the gain of encryption and decryption. This was used in Transport Layer Security, HTTPS for encryption, decryption gain.

So, we are introducing this technique to improve the encryption, decryption gain and messaging scheme in VANET. It is light and efficient Secure Hybrid (SH-RSA) communication scheme that is studied and implemented with a four-layer authentication stack. The problem solving in RSA was associated with a very low speed while decrypting messages.

This complexity of computational mobile (modular) exponentiation and a partial vulnerability problem of exposure in RSA. Not only does it address various RSA scientific problems, It also uses 2% — 4% less CPU than the main RSA and only 1% — 3% less space than the main RSA. This was found under the scheme's analysis and changes.

II. PROBLEM STATEMENT

VANET safety tackles concerns related to encryption, privacy such as identification and location of vehicles. At the same time, the traceability of authorized vehicles is important because a trusted authority (TA) must disclose a vehicle's identity so that its operator can never challenge the authorship of an accepted text[2]. VANET has introduced different types of approaches to tackle privacy and security issues in order to align confidentiality, authentication and revocation requirements[9]. All in all, the nom de plume been regularly used to acquire unknown correspondences and secure the protection of vehicles, and there are a scope of strategies for pseudonymity dependent on simple cryptography[4]. Symmetric key cryptography arrangements are computationally productive, yet they are normally not proper for delicate vehicle-to-vehicle interchanges as vehicles need contact the base station to decode messages from another vehicle. In order to remove the need for public-key certificates, systems are proposed based on identity-based cryptography which exploit the implicit authentication given by identity-based cryptography to produce unforgettable pseudonyms[9].

III. RELATED WORK

The SH-RSA informing plan for VPN and LAN to LAN situation is the consequence of the principle RSA.

This allows the user to address dangerous known plaintext attacks, resulting in stronger and more statistical complexity and also it guard against multiplicative property manipulation[1].

Mysterious certifications have additionally been reached out to vehicle correspondences, Furthermore, there are conventions utilizing credit based validation to accomplish vehicle interchanges get to control, however they face difficulties emerging from supplanting nom de plumes characteristics for vehicle ID[6].

The existing messaging scheme in vanet has many techniques which takes longer time to encrypt and decrypt the text message that needed to communicate between the two vehicles[1]. The existing system lacks the secure communication for vanet. Leakage of travel Routes breaches the privacy of Drivers and may have serious consequences, as such that routes may used for crimes. Such messages need to be protected while communicating [9].

IV. PROPOSED SYSTEM

The Secure Hybrid (SHRSA) lightweight and effective. It is a four-layered authentication store communication system that needs to be applied and evaluated. Since it guard against multiplicative property manipulation [1] we are proposing A Secured Hybrid RSA (SH-RSA). This four-layer authentication stack has stalked the username, electronic certificates, and 3rd party for authentication using the four-layer techniques of its own.

This is used mainly to solve problem of encryption, decryption speed and messaging scheme. The more encryption of four layers eliminates any third party and applies only to private messaging. Each authentication provides the basic security for the messaging services, while SH-RSA provides a secure connection between any two individuals. This will be done with the help of the Four-Layered in the Secure Hybrid RSA. This multi-layered communication system provides security that will be carried from one end to the other [11]. This encryption scheme is applied in a stalked fashion under the four techniques. The main difference in SH-RSA is that decryption efficiency has an 8.53-fold gain relative to the original RSA, while it also has more gain than CRT-RSA. Let's discuss about the four layers:

3.1.1 Layers of SH-RSA:

It's basically designed with a unique IP address with the help of "Trusted Third Party" [TTP].It acts as an exchange key in SH-RSA.

Layer 1, the methodology of having a SH-RSA server with n number of SH-RSA schemes connected into it. Through P2P authentication 2 users can communicate by sending messages and could not initiate the messaging process. This is a pure P2P authorized messaging scheme which connects with them through a unique IP address for every connection.

Layer 2, this is a 3 way handshaking process between the friend. This principle module is by utilizing Diffie-Hellman Key which trade convention for layer 3 of every 4-layered verification stack. We are utilizing PFS grade 4 - Older Diffie-Hellman in layer 4 without bends. It is a special property which won't arrange any concur key.

4 Stacked designs that evacuate the personality discharge switch. On the system layer, IP sec running on the system layer can be utilized in any vehicle layer by IP sec guaranteeing the protection and security of the IP payload by utilizing the IP header trustworthiness in addition to payload utilizing (AH) convention and the typified Security Payload convention.

Application developers ' efforts to facilitate IP sec on IPv6 h osts have already been applied by device vendors on the net work layer. IPsec is excessively mind boggling and has numerous highlights with numerous alternative IPv6 is required in the IPv6 convention, this encourages at untouched, all IPv6 is a prepared gadget which have the IPsec arrangement as default.PFS is one of a kind property's bit of leeway

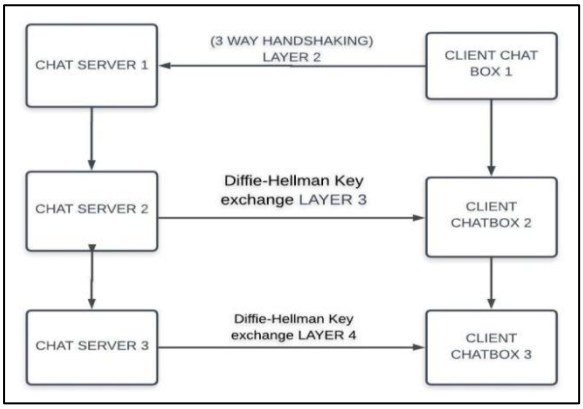

Fig:3.3.1 Four layer Authentication

The advantages of SH-RSA informing plans are:

1. Secure mixture RSA encryption process depends on start to finish encryption, which makes the message increasingly secure and keeps the CIA (Confidentiality,Integrity and Accessibility) group of three secrecy.
2. The two key is utilized for encryption and decoding, no need of a different key for the unscrambling of the parcel information (content) in the bounce PC on the system.
3. For More secure E2E encryption is utilized for case delicate to shield it from security assaults.
4. For high modularization of the usefulness is conceivable in SH-RSA informing plan.
5. The file size required for SH-RSA informing plan is under 0.25kb, and the informing procedure in SH_RSA utilizes extremely less time for encryption.

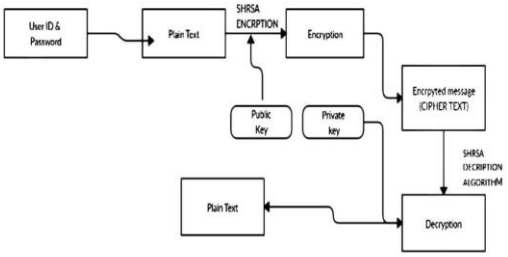

Fig:3.2.1 Architecture Diagram

3.2 ALGORITHM FOR SH-RSA

i) Pick prime numbers a = 3 and b = 11
ii) Compute x = ab and z = (a – 1)(b – 1)
x = ab = (3)(11) = 33
z = (a – 1)(b – 1) = (3 – 1)(11 – 1) = (2)(10) = 20
iii) Pick a number e < x it ought not have normal variables with z other than 1.
Let e = 7
iv) Discover number D with the end goal that ed divided z has a rest of 1. Utilizing expanded Euclidean calculation discover opposite modulo 33 find:
d = 3.
v) The Public key K + B the number pair [x, e] and private key becomes KB or (x, d)
Thus, Encryption formula : c = me mod x
This produces encrypted value of the Plain text "check" as 8 10 17 17 15 where: c ! 3 h ! 8, e ! 5, c ! 3, k ! 11. In order to decrypt the message
Decryption formula-- m = cd mod x
Decryption provides the plain text: "CHECK"

V. RESULT ANALYSIS

The main goal is to build a model of application related to safety. It provides the project with security code and performance. A four-layered theory called "SH-RSA" which provides users with a secure communication similar to other messaging scheme methods and a time taken for encryption and decryption is fast. It is based on true encryption with E-2-E. It improves the system's authenticity. This four-layer authentication stack is primarily used to solve the problem of decryption speed, modular math and exponentiation difficulty.
The encryption , decryption gain has various performance in RSA, RSA-CRT and SH-RSA. RSA performs more encryption and decryption gain compared to RSA-CRT. The advanced version of RSA called SH-RSA produced more encryption, decryption gain among all the techniques. SH-RSA consumes only 500 time in milli-seconds. This running comparison shows the gain of SH-RSA.

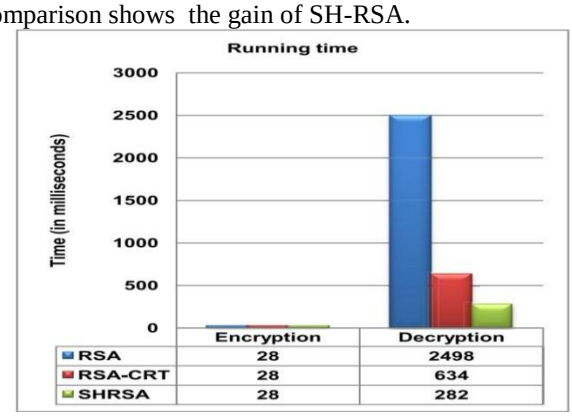

Fig:4.1 Running time comparison of RSA and SH-RSA

VI. CONCLUSION

VANET is used to ensure safety while travelling on roads by broadcasting safety messages from one vehicle to another vehicle. The strong security method implemented to handle several security attacks. Even though there is many messaging scheme techniques it is observed that many security issues need to be sorted out. So, here the new messaging technique SH-RSA used for vanet which provide more security compared to recent messaging schemes. This technique provides safety for many attacks such as spoofing attack, provides e-2-e security. And the time taken to the encryption , decryption process is faster compared to other techniques. So, SH-RSA Authentication technique for VANET will satisfy all the security and provide secure messaging between vehicle to vehicle.
The future enhancement is based on the Resurgence of Physical-Based Security. Privacy in messaging scheme will be increased. The user messaging scheme needs to be one that combines of use with security. This Encryption will be changed in the future, according to the encryption , decryption gain, a physical based technique is used in the future.

REFERENCES

1. A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack Aniruddha Bhattacharjya , Xiaofeng Zhong, (Member, IEEE) AND Xing Li. 2019
2. M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," Ad Hoc Netw., vol. 8, no. 7, pp. 778–790, 2010.
3. Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," IEEE Commun. Surveys Tuts., vol. 10, no. 3, pp. 74–88, Third Quarter 2008.
4. D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 12, pp. 2681– 2691, Dec. 2015.
5. M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Commun., vol. 13, no. 5, pp. 8–15, Oct. 2006.
6. J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," IET Commun., vol. 4, no. 7, pp. 894–903, 2010.
7. J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.
8. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.
9. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc.27th Int. Conf. Comput. Commun., Apr. 13–18, 2008, pp. 1903– 1911.
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.27th Int. Conf. Comput. Commun., Apr. 13–18, 2008, pp. 816–824.
11. T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad

AUTHORS PROFILE

Jack Shelton J, 3rd year student of B.tech CSE from SRM Institute of Science and Technology, Chennai

Ashwin kumar R, 3rd year student of B.tech CSE from SRM Institute of Science and Technology, Chennai

Bhuvanesh K, , 3rd year student of B.tech CSE from SRM Institute of Science and Technology, Chennai

Ms. M.S Bennet Praba, Assistant Professor, Computer Science Engineering Department in SRM Institute of Science and Technology, Ramapuram, Chennai