Performance Analysis Of Authentication And Efficient And Secure Message Communication In Vanets

Shaji. K. A. Theodore

Abstract: A wireless environment demonstrates a vital role during the past years in the communication world. Wireless connection is a core area in Mobile Ad hoc Network (MANET). Vehicular Ad hoc Network (VANET) is an emerging field of MANET in such an instance a vehicle performs as a nodule transmitter with remaining vehicles and highway transportation in the networking system. For enhancing secure driving, they assured to provide upcoming safety crucial progressive mechanisms for the driver aid system. As a result of wireless information sharing, attacks gone through with fewer attempts and protection and privacy of persons involved in such networks are the key aspects. Through wireless media, every vehicle will message (Msg) with each other for safety Msg transmission and keep updated with risk and traffic conditions. The Security goal is preventing third parties disclosing incorrect information in the network, which gives rise to misfortunes and is a significant feature in secure messaging. In this paper, Elliptic Curve Cryptography (ECC) produces a key for the vehicles in which RSUs operate as a Certificate Authority. This paper investigation established that the whole Msg size impact on VANET messaging system and communication link protocol investigation conducted for performance measuring in a VANET message transfer system.

Index Terms: VANET, Cryptography, MANET, Authentication, Security, Communication, Encryption, Decryption .

1. INTRODUCTION

THE mobile node grouping is endangered by MANET [1] disseminated excluding of infrastructural development and has the self-assembled ability in a distributed approach. The global investigators exhibit a tremendous interest in VANETs [2] because it is a field of emerging technology. It is an innovative area of movable network administrator that has the ability of a self-production network in a distributed approach with a small infrastructure plan. For secure transmission in VANET, security is a significant feature. The Protocol, which is securely transmitting information complying with operational demands primarily because security-related applications also have demanding functional needs. The extent of this research confined to VANET functions that are security sensitive and provides direct communication between more than single vehicles. Moreover research paper describes core safety functions are initially described, evaluating guaranteed protocol communication to check whether they met the performance necessities required by security related applications [3]. The whole Msg size is described by Msg load capacity and unencrypted operating cost expenses by the safety associated technique. By assessing the effectiveness of verification protocols comprises by evaluating the total Msg size and message transfer on Msg waiting period, production capability of the channel, Msg completion time, and its impact on security related applications and protocol verification. Moreover examined that protocol authentication handles safety demands of secured applications [4]. The existing researchers proposal provided are consistent and well-organized and their large number of proposals verifies to be accurate and extraordinary.

• *Shaji. K. A. Theodore, Faculty Information Technology, Al Musanna College of Technology, Oman.*

In this work, various contributions are made in VANET security although having several faults:

1. At the receiver and sender side, communication verification delayed.
2. The MSG transmission cost at both the sender and receiver side.
3. As a result of the encoding and decoding of the Msg, data processing rate increased. Continually upgrading the checklist of invalidated nodes and transmitting to the whole set of nodes in the network directs to a high estimation rate.
4. Amount of memory required for the restoration of the upgraded revoked list and memory needed for each pseudonym for accumulating and assuring.

Inspired from this entire research paper, here, a protocol propounded that acquired advantages through the current protocol moreover perform the enhancement in the present research area to attain safety, confidentiality, and validation towards entire issues [5]. This research work enables supplying the data, validity of data, consistency, non-denial, and effectiveness.

Our suggested research work has maximum security when compared with other work because, by the utilization of ECG, it obtained the key of 160 bit, and in the proposal, RSA utilized 1024 bit, however, employed with fewer key sizing. Compared with RSA, ECDSA has a high level of assurance. ECC involves less storage space than others. Moreover, it leads to guaranteed security since ECDLP has greater security when compared with IFP and DLP [6].

Section 1 describes the motive of this research paper. Section 2 performs a brief analysis of MANETs, and the final part mainly resides on the application, uniqueness, and high-technology related to VANETs. In section 3, VANET features investigated, and safety-significant V2V applications are recognized and scheduled. Section 4, a protocol assessment, implemented for calculating computation overheads and cryptographical properties examined. Section 5 provides final comments on protocol examination and performance analysis.

2 RELATED WORKS

The MANETs source in 1972, traces back to DARPA Packet

Radio Network Project. Moreover, examination in MANETs restricted to armed forces for a while, whereas in 1990, with the introduction concerning business broadband regulations, the capability of MANETs started to be intercepted outside the military. A protocol propounded is significant in Distributed Certificate Service (DCS) [7] system in automotive ad-hoc networks. The planned proposal provides flexible compatibility for certification work in different directorial administration and an efficient path for pre-loaded elements similar to OBUs to restructure confirmation by utilizing available structure Roadside Entity (RE) inappropriate approach. Furthermore, the method of DCS provides a complete cluster verify approach for validating verification underlying imprints, fundamentally reduces the authentication expense. Secure and performance assessment demonstrates the DCS [8] plan and reduce difficulty in certified administration and achieve unbelievable safety and competence in Msg transmission for vehicles. An authentication management concept of zone wise based on judiciary limits and organizational described. Its objective is to mishandle the geographical region of automobile communications to reduce the difficulty with the authentication structure of PKI based. The Effective Conditional Privacy Preservation (ECPP) [9] protocol projected and primary procedure that offers assistance for a fit motor vehicle to re-establishing a Pseudonym record for a short period from the RSUs rapidly. We have observed a vital study effort by the administration, academic world, and business to incorporate data processing and technological communication into vehicles that enabled the progress of Intelligent Transportation Systems (ITS) [10]. In ITS, Vehicular Communication (VC) is a vital module where automobile vehicles interact with other vehicles and highway transportation, examine and development, by analyzing decision making.

3 PROPOSED METHODOLOGY

In this research proposal, we believe that the path is protected and mostly concerned with the verification and reliability of Msg. Msg authentication is the principal work that should be received from authentic vehicles and the necessity of securing Msg that nobody can modify the Msg. We suggest a representation of the secure validation and reliability of Msg in an adversarial atmosphere. In this paperwork, initially create the key for Msg encoding and decoding. Public and private keys generated by the asymmetric key generation algorithm. From the certification authority, two keys are made, and an additional algorithm [11] utilized for transmission, and the generated keys are also used for this transmission function. The complete design partitioned into two steps. The primary level is enrollment, and the following is Transmission.

3.1. VANET Set-up

Every time if the vehicle goes through the VANET and needs to converse with other vehicles, that they need to perform enrollment with certifying authorities. In this level, keys generated for every vehicle. We suggested the highway department as certifying authorities utilized for vehicle registration. The Enrollment phase, mostly handled by a public key environment system for certifying authorization, offers the public and private key to the automobile transmission method indicated in figure 1.

3.2. Msg Communication Stage

The vehicle - VANET-I and VANET-II would like to converse with each other, and vehicles need to maintain the legitimacy and reliability of their Msg(s). For security purposes, this level utilized Elliptic Curve Diffie Hellman (ECDH) method [12]. ECDH is a protocol concerning dual vehicles shared secret code in a private key algorithm. Since both vehicles sharing private Msg with public data in an attacker atmosphere, dual vehicles compute the confidential secret code; on the other hand, the other vehicles cannot compute secret code as they don't have the secret information hence transmission is secured.

3.3. Procedure for Registration

Pub and PrKey generation for a vehicle gone through four stages from certifying administration is RSU.

Step 1: Presume a motor vehicle V-I makes a request for Msg for PrKey to the certifying authority in encoded format. The encoding completed with the pubKey of the certifying authority and request Msg enclose ID of driver "X," ID of vehicle V-I, area factor for Elliptic Curve (EC), and time stamp [13].

EncKey (CertA) [IDX||IDV-I|| (P, x, y, Gen, N, H) ||N-I] …….(1)

Step 2: Currently, CA would send the private key "d(X)" to the vehicle V-I in the encoded format with the ID of driver "X."

EncKey (CertA) [IDX||d(X)] ……(2)

Step 3: Yet again, the vehicle V-I send a request Msg for the generator (Gen) to the certification administration and request Msg hold the ID of "X" with time stamp encoded with the private key of "X" that once more encoded with the public key of CA [14].

EncyKey (CertA) [EncyDecy (X) [IDX|| N-II]]……..(3)

Step 4: At this time, the CertA would send the Gen to vehicle V-I with the ID of X and time stamp encoded with PubKey of CA that one more time encoded with PrKey of X.

EncyKey (CertA) [EncyDecy (X) [IDX || N-II || Gen]]…….(4)

Step 5: Currently, Vehicle V-I contains both PrKey "Decy(X)" with Gen by which he computes his own PubKey P(X).

P(X) = Decy(X)*Gen……(5)

Step 6: Correspondingly, vehicle V-II acquire its Pub and Prkey from Certification Authority, so, in the last part of the registration stage, both vehicle V-I and V-II contain PrKey and PubKey.

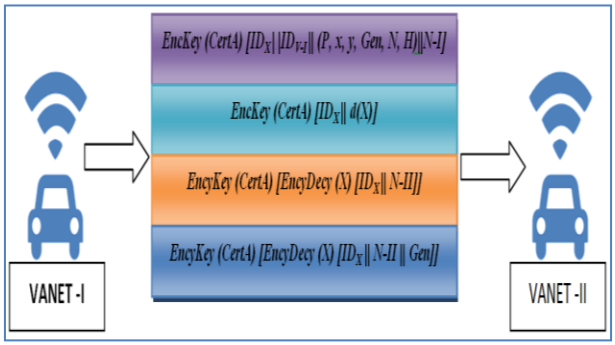

***Figure 1**. VANET Set-up*

3.4. Communication Route

In this process, the vehicles (V-I, V-II) should accept on ECC Domain variables for producing a confidential, secret code and two motor vehicles having its own public and private key pairs [15]. Assume V-I has a key pair (Decy(X) & P(X)) where Decy

(X) is PrKey, and P(X) is PubKey of V-I. Likewise, V-II encloses key pair (Decy (Y) & P(Y)) where Decy (Y) is PrKey, and P(Y) is PubKey of V-II (refer figure 2).

The secret code creation as follows:

If V-I → PubKey PY Then

Compute V-I = K= Decy (X)*P(Y)

End If

Else IF V-I → P(X) and V-II Then

L= Decy (Y)*P(X)

P(Y) = D(Y)*G and P(X) = Decy (X)*G

Decy (X)*P(Y) = Decy (X)* Decy (Y)*G = Decy (Y)*d(X)*G = Decy (Y)*P(X)

where, k = L; $X_K = X_L$; X_K = Shared Secret Code of V-I and V-II

End if

***Figure 2**. VANET Msg Communication*

4 Performance Analysis of Authentication

Both of these situations, roadways, and overcrowding addressed for performance reviews. The number of parametric values of both conditions provided in Table 1, taken from the Value of Msg sizes, is preferred to communicate to a maximal Msg size of 1200 bytes, according to the selected Msg range. The minimal DSRC [16] [17] communication capability of 5 Mbps for secured Msg(s) taken into consideration. In both situations, indicates, motor vehicles are movable then transfer DSRC Msg(s) in l ms in the course time. In consideration of a vehicle V I/II positioned in the highway median, it can receive maximum Msg(s); V I/II can listen to n motor vehicles for every 0.01 ms. In the worst-case scenario, encompassing whole motor vehicles struggle for the channeling, the output is T, it assumed that the minimum rated output of DSRC is 5 Mbps. Before sending V I/II to a novel Msg, they would be capable of operating inbound Msg transmission Msg(s) in 0.01 ms. It implies that V I/II accept complete N Msg(s) (even though the mean reception rate is lesser than 1, the upper limit is expected). Moreover, in a roadside situation, consider a single-track with communication range limit of 300 m, a vehicle can have the sense of hearing 15 vehicles/ Msg(s) (communication rate segregated by inter-regional distance of vehicle) [18] in the traffic center from forward and ten vehicles / Msg(s) as of the back (overall 20 in every track), for each signal. For 4 lanes, motor vehicles population computed as N = 22 * 5 = 110. Likewise, in the jamming situation, N = 48 and R = 22 is calculated by imagining a motor vehicle perceive sound in all traffic in its limits (upper limits).

***Table 1**. Scenarios of Network Congestion*

Parameters	Roadway	Congestion
Vehicle Speed	>20	<20
MSG Size	50,100,150,200	50,100,150,200
No. of MSG Received	130 per 250 ms	50 per 150 ms
MSG Range	350	50
Latency	35	10

The selected protocols require PKI and Group Signatures (GSign) for employing VANET, hence significant to prefer a PubKey Cryptosystem (PKCS) and GSign in satisfactory accomplishment overhead expenses in the automotive environment. This portion analyzing efficiency by Elliptic Curve Digital Signature Algorithm (ECDSA1) and the GSign projected in Table 2. The fundamental elements utilized for cryptography functions are BP, GS, and HS.

***Table 2**. Computational Cost and Overheads*

Cryptographic Algo.	Security Level	PubKey	Verification Time	Sign
ECC	128	35	4.7	62
GSign	80	289	21.18	189

In DSRC, securities associated Msg(s) throwing with regular intervals of 100 to 300 ms. It enforces a higher limit for handling time operating cost as follows:
where Timesign(Msg), TimeTX(MjSigPrKey [Msg]); and Timecheck(Msg) are the essential time period to sign, transfer, and confirm a Msg, correspondingly. As of expression (6), we observe processing time that relies on signing and signature authentication. To facilitate the significant processing time of a specified PKCS is the signature authentication time because every motor vehicle regularly obtains numerous Msg(s) for verifying purpose while signing and send only one Msg at the same time (figure 3 (a)(b)(c)(d)).

$$Time(Msg) = Time_{Sign}(Msg) + T_{TX}(Msg \mid Sign\,\mathrm{Pr}\,Key(Msg)) + Time_{Check}(Msg) \quad \text{.....(6)}$$

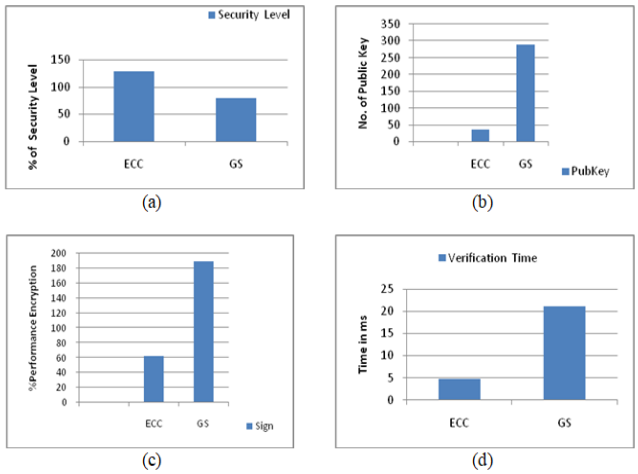

***Figure 3.** (a) Security (b) Key Selection (c) Signature Impact (d) Verification Time*

4.1. Total Msg Size vs. Communication Throughput

The VANET system output described by the bandwidth, which is required by automobile in the transmission channel and computed as follows.

$$ThroughPut = \frac{NXRXMsgX8}{2Mbps} \quad \text{.....(7)}$$

The overall Msg size Msg = S + O: For e.g. in BP Msg =S+138 bytes. In GSing method, the overhead Msg =S+225 bytes. In Hybrid scheme, Msg = S + 298 bytes. Different Msg sizes have selected for analyzing Msg performance. The diverse values of s replaced within equation 2 for highway (N=125, R=3.13) and congestion (N=37, R=10.12) situation. Table 3 provides different throughput values (equation 7) for various Msg sizes under different validation methods.

***Table 3**. Performance authentication measures of congestion vs. throughput*

Scenario	Msg Size			
	50	100	150	200
Throughput	0.62	1.10	1.75	2.34
Congestion	0.91	1.16	1.99	2.71

By the simulated outcomes, we observe that a total Msg size of 100-300 bytes is perfect for secure messaging (drastic Msg losses after 300 bytes). HS has an overhead of 298 bytes, and the whole Msg size readily exceeded 300 bytes. For a specified Msg size, the better alternative for the validation method is to reduce Msg losses and to decrease BP output (figure 4)

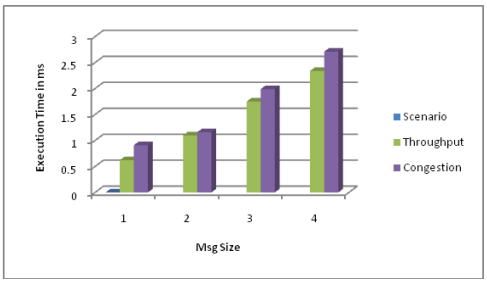

***Figure 4**. Performance of congestion vs. throughput*

4.2. Total Msg Size vs. Msg Delay

The amount of time required to convey Msg from sender to receiver refers to Msg delay. In accordance with, the average Msg holdup has considerable differences while the Msg size increased since fewer struggles scheduled on the standard and the high transition speed reduce Msg size effect. In various situations, the highest Msg delaying acquired calculated in table 4.

***Table 4**. Msg Size vs. Delay*

Overall Msg Size (bytes)	Msg Delay – Max.(ms)	Msg Delay – Min. (ms)
50	10	15
90	25	28
120	39	40
150	45	49
240	55	51
350	69	59

In Table 3 for another request, the highest acceptable waiting time is 100 ms. The values obtained below this upper limit. Expecting similar Msg delay values for BP, GS, and HS, these methods utilized for real-time applications.

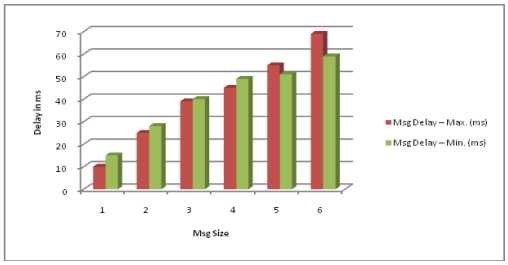

***Figure 5**. Performance of Msg Size vs. Msg Delay (Min-Max)*

4.3. Messaging Processing Rate vs. Processing Time Delay

Processing time per Msg described by the amount of time required for vehicle to authenticate for every Msg it accepts. The processing time differs from the message transfer rate, as described below (EQU (8)).

$$Delay = \frac{Latncy}{No.ofVANETs} \quad \text{.....(8)}$$

• Condition of Public Road: In this situation, latency=300 ms and vehicles no: N=120. As a result of the highest acceptable processing delay=300=120=2.5 ms. At this moment, every vehicle has a maximum 2.5 ms for Msg processing among successive Msg(s).

• Congestion: In this, latency=100 ms and number of vehicles no: N=36. Thus maximum tolerable processing delay=100=36=2.78 ms. Each vehicle has the highest of 2.78 ms for Msg processing.

As a final point, we generated ECC encoded with java language into Net beans editor then compiled and executed in java platform. The computation time for ECC encoded execution time is 1.21 sec. In this research work, the encryption technique utilized for four times, so the total computation time taken for execution is = 1.21 sec * 4 = 4.84 sec.

5 Conclusion

In this research paper, our core objective is a useful model designing and safe Msg transmission in VANET. The automobile applications classified, and the significance of security-related applications and their architecture have developed. A model designed for communication and registration process for secure Msg transmission. For the registration phase, ECC utilized by providing Pub and PrKeys for the corresponding vehicle, and in the communication phase, ECDH is employed by sharing secret code for data transfer between the vehicles. This propounded model attains low transmission and data-processing costs with less size with enhanced security by the usage of ECC and ECDH. The foremost intention of this paper is to investigate the cryptography cost consequences, overall Msg dimension, and message transfer rate on effective Msg transfer communication in secured protocols, for V-2-V security-related applications.

ACKNOWLEDGMENT

NA.

REFERENCES

[1] T. Song, W. W. Xia, T. Song, and L. Shen, “A cluster-based directional routing protocol in VANET,” in Proc. IEEE ICCT, pp. 1172–1175, 2010.

[2] Vinel, “3GPP LTE versus IEEE 802.11p/wave: which technology is able to support cooperative vehicular safety applications?,” IEEE Wireless Commun. Lett., vol. 1, pp. 125–128, Apr. 2012.

[3] A. Moller, J. Nuckelt, D. M. Rose, and T. Kurner, “Physical layer performance comparison of LTE and IEEE 802.11p for vehicular communication in an urban NLOS scenario,” in Proc. IEEE VTC, pp. 1–5, 2014.

[4] A.Ghosh, J. Zhang, J. Andrews, and R. Muhamed, Fundamentals of LTE. Pearson Education, 2010.

[5] D. Meyer, “AT&T speeds up connected car business,”

RCR Wireless, Feb 2016.
[6] Kerns, K. Wesson, and T. Humphreys, “A blueprint for civil GPS navigation message authentication,” in 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014, pp. 262–269, IEEE, 2014.
[7] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, “Position-based quantum cryptography,” arXiv preprint arXiv:1005.1750, 2010.
[8] M. Mirshahi, J. T. Obenberger, C. A. Fuhs, C. E. Howard, R. A. Krammes, B. T. Kuhn, R. M. Mayhew, M. A. Moore, K. Sahebjam, C. J. Stone, et al., “Active traffic management: the next step in congestion management,” Tech. Rep. FHWA-PL-07- 012, Federal Highway Administration, July 2007.
[9] Florian Dötzer, Markus Straßberger, and Timo Kosch. Classification for traffic related inter-vehicle messaging. In the 5th International Conference on IST Telecommunication. BMW Group Research and Technology, Germany, Jun 2005.
[10] S. Eichler. Performance Evaluation of the IEEE 802.11p WAVE Communication Standard. Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, pages 2199–2203, Oct 2007.
[11] James A. Freebersyser and Barry Leiner. A DoD perspective on Mobile Ad Hoc Networks. Ad Hoc Networking pages 29–51, 2001.
[12] Zygmunt J. Haas, Joseph Y. Halpern and Li Li. Gossip-Based Ad Hoc Routing. IEEE/ACM Trans. Netw., 14(3):479–491, 2006.
[13] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, Ta- Vinh Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. IEEE Communications Magazine, 46(11):110–118, 2008.
[14] Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues," IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 74-88, 2008.
[15] S. Zeadally, R. Hunt, Y. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2010.
[16] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, “Provably secure identity-based signcryption scheme for crowdsourced industrial internet of Things environments,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2904–2914, 2018.
[17] L. Zhang, Q. Wu, J. Domingo-ferrer, B. Qin, and C. Hu, “Distributed aggregate privacy-preserving authentication in VANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017.
[18] L. Zhang, X. Men, K. K. R. Choo, Y. Zhang, and F. Dai, “Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud,” IEEE Transactions on Dependable and Secure Computing, p. 1, 2018.