Security Mechanism for Emergency Messages of Vanet Cryptography Schemes

Pitty Nagarjuna

Abstract-- My invention "Further developed Security Mechanism for Emergency Messages of Vanet Cryptography Schemes.)" Vehicular Ad-hoc network (VANET) is one of the emerging advancements for research neighborhood get different assessment ***challenges*** to assemble got framework for free vehicular correspondence. The incredible concern of this development is to give capable data correspondence among enlisted vehicle centers. The couple of investigation considerations are executed in every practical sense, to deal with all around correspondence in VANETs by contemplating security and insurance as critical pieces of VANETs. A couple of instruments have been done using cryptography computations and procedures. Anyway, these instruments offer a response just too a few bound conditions and to confined security risks. From this time forward, the proposed novel framework has been introduced, executed and took a stab at using key organization technique. It gives secured network environment to VANET and its parts. A while later, this part gives security to data heaps of emergency messages using cryptography instrument. From this time forward, the proposed novel part is named Group Key Management and Cryptography Schemes (GKMC). The exploratory assessment shows tremendous improvements in the association execution to give security and insurance to emergency messages. This GKMC part will help the VANET clients to perform gotten emergency message correspondence in network environment.

Keywords -- Security, Mechanism, Emergency, Messages, Vanet, Cryptography Schemes.

FIELD – My invention is related to an Improved Security Mechanism for Emergency Messages of Vanet Cryptography Schemes.

I. INTRODUCTION

The transportation framework assumes a significant part in the improvement of any country's monetary development. Accordingly, the interest for vehicles increments. This expanded use of vehicles enjoys a few benefits like better and proficient transportation, and furthermore it has a few impediments identified with street wellbeing and different issues like mishaps. A new report uncovered that, a sum of 232 billion mishaps are accounted for in the United States and 100 thousand passing’s are accounted for consistently in China, and it is as yet expanding.

In these mishaps, over 57% of mishaps are caused because of human mistake like absence of consideration, helpless participation among vehicle drivers and helpless choices. The continuous trade of mishap caution between vehicles can assist with keeping away from these occurrences. This correspondence between vehicles can be performed utilizing remote correspondence. As of late, expanded development of remote correspondence has acquired tremendous fascination in different ongoing applications like portable correspondence, remote sensor organizations and satellite interchanges, and so on.

The innovative development in systems administration, implanted innovation has empowered different improvement openings for the car business because of that vehicles are furnished with different kinds of savvy gadgets like Wi-Fi, GPS and other brilliant gadgets. Because of these keen gadgets, vehicles can convey each other through remote organization and works with the development of Vehicular Ad Hoc Network (VANET) where vehicles can impart to stay away from clog and mishaps.

As of late, various explores are directed to the foundation of solid Intelligent Transport System (ITS) which has a few offices, for example, traffic checking, crash control, traffic stream control, close by area data administrations, and web accessibility in vehicles. For the most part, VANETs are portrayed by the accompanying components like unique organization geography, on-board sensors, limitless force, and capacity, and so forth Additionally, the VANET correspondence frameworks can be characterized dependent on the correspondence types which are: Intravehicular correspondence inside the vehicle, vehicle to vehicle correspondence (V2V), vehicle to foundation (V2I) and mixture correspondence (V2X) where a vehicle can impart to the vehicle and street side units (RSU).

During the last decade, the advancement of ITS and VANET have acquired consideration by research, modern and scholarly field because of its promising nature of solid transportation framework. A few kinds of examination have zeroed in on this field and created different ways to deal with work on the exhibition of VANETs. Notwithstanding, this correspondence is performed utilizing remote correspondence engineering where directing is viewed as a difficult errand. VANETs have a few applications which are basically sorted into two classifications like, security and non-wellbeing applications. The wellbeing applications perform communicating security messages and cautioning messages for helping the street to forestall mishaps.

Pitty Nagarjuna, *-Principal Research Scientist, Indian Institute of Science, Bengalore 560012, India

https://doi.org/10.17758/EIRAI18.F0523108

These messages can incorporate different kinds of data like street mishaps, gridlocks, crisis vehicles, and street development, and so on.

II. OBJECTIVES

The objective of the invention is to provide a “Improved Security Mechanism for Emergency Messages of Vanet Cryptography Schemes.)” Vehicular Ad-hoc network (VANET) is one of the arising innovations for research local area to get different examination difficulties to build got system for independent vehicular correspondence.

The other objective of the invention is to provide a great worry of this innovation is to give proficient information correspondence among enrolled vehicle hubs. The few exploration thoughts are executed for all intents and purposes to work on by and large correspondence in VANETs by thinking about security and protection as significant parts of VANETs.

The other objective of the invention is to provide a few instruments have been carried out utilizing cryptography calculations and strategies. In any case, these instruments give an answer just to some confined conditions and to restricted security dangers. Henceforth, the proposed novel system has been presented, executed and tried utilizing key administration method.

The other objective of the invention is to provide a gives tied down network climate to VANET and its parts. Afterward, this component gives security to information bundles of crisis messages utilizing cryptography instrument. Henceforth, the proposed novel component is named Group Key Management and Cryptography Schemes (GKMC).

The other objective of the invention is to provide a exploratory examination shows huge enhancements in the organization execution to give security and protection to crisis messages. This GKMC component will help the VANET clients to perform gotten crisis message correspondence in network climate.

III. SUMMARY

As of late, various explores are directed to the foundation of solid Intelligent Transport System (ITS) which has a few offices, for example, traffic checking, crash control, traffic stream control, close by area data administrations, and web accessibility in vehicles. By and large, VANETs are described by the accompanying components like unique organization geography, on-board sensors, limitless force, and capacity, and so forth Additionally, the VANET correspondence frameworks can be arranged dependent on the correspondence types which are: Intravehicular correspondence inside the vehicle, vehicle to vehicle correspondence (V2V), vehicle to foundation (V2I) and crossover correspondence (V2X) where a vehicle can convey to the vehicle and street side units (RSU).

During the last decade, the improvement of ITS and VANET have acquired consideration by research, modern and scholastic field because of its promising nature of solid transportation framework. A few kinds of exploration have zeroed in on this field and created different ways to deal with work on the exhibition of VANETs. In any case, this correspondence is performed utilizing remote correspondence engineering where directing is viewed as a difficult assignment. VANETs have a few applications which are basically classified into two classifications like, security and non-wellbeing applications. The security applications perform sending wellbeing messages and cautioning messages for helping the street to forestall mishaps. These messages can incorporate different kinds of data like street mishaps, gridlocks, crisis vehicles, and street development, and so forth.

This segment presents the proposed model for secure and proficient correspondence in vehicular Ad-Hoc organizations. The huge measures of works have been completed to further develop correspondence execution yet security stays a difficult undertaking. In addition, the unique organization geography makes a few testing issues. In this manner, client validation and key administration will be a drawn-out errand to keep up with the fix correspondence. This examination work is zeroing in on key administration and information security. The proposed model of GKMC coordinated as follows:

A. First of all, we convey a Vehicular Ad-Hoc arrange and characterize the primer and introductory suppositions identified with the organization.

B. In the following stage, V2V, V2 and V2X correspondence convention is introduced where key administration, verification, key trade modules are introduced.

C. Finally, the cryptography plot is introduced to get the information parcels.

Gathering Key Management

This work initially portrays the bilinear guide age to join the security usefulness in the organization. Allow us to think about that $\mathcal{G}o$ and $\mathcal{G}N$ are the added substance cyclic gathering with the enormous prime request $\mathscr{p}$. A guide work F is processed as in condition 1.

$$\hat{F}\colon \mathcal{G}o \times \mathcal{G}N \rightarrow \mathcal{G}N \qquad (1)$$

In which it should satisfy the following conditions to generate the bilinear pairing.

Bilinear: for all M, $N \in \mathcal{G}o$ and for all a, $b \in \mathcal{Z}\mathscr{p}*$, the function is $\widehat{F}(aM, bN) =$ $\hat{F}(aM,\ bN)ab$. Similarly, for all M, N, $\in \mathcal{G}o$ the bilinear map as in equation 2 and 3.

$$\widehat{F}(M+N\ ,Y) = \widehat{F}(M,Y)\widehat{F}(N,Y) \qquad (2)$$

$$\hat{F}(M,\ N+Y) = \hat{F}(M,\ N)\hat{F}(M,\ Y) \qquad (3)$$

Non-degenerate: there exists that the M, $N \in \mathcal{G}o$, there is $\hat{F}(M + N\ ,\ Y) \neq 1$

Computability: for all $M, N \in \mathcal{G}o$efficient approach is present to compute the $\hat{F}(M, N)$

Symmetric: As per equation C4 for all $M, N \in \mathcal{G}o$

$$\hat{F}(M, N) = \hat{F}(N, M) \tag{4}$$

As per the proposed approach first, it addresses the verification cycle among RSU and vehicle. The total verification measure is separated into three stages as introduction, validation and conveyance of gathering keys. The functioning system of these stages is depicted in the accompanying subsections.

Initialization

In the initial step of proposed GKMC approach, we perform client enrollment and key assignment for every vehicle in the organization. In VANET engineering, a vehicle should be enlisted with the TA then TA doles out restricted intel to the comparing vehicle. During this cycle, the TA stores driver data, for example, contact data, address and tag number. Allow us to consider that the $G\mathcal{H}$ as cyclic added substance bunch, $Q\mathcal{H}$ is the generator and remarkable vehicle id is meant as id. Here, we take on the Hash work as where signifies the nonnegative number set which is not exactly the indivisible number $\mathscr{p}$. In view of these presumptions, the TA produces a mysterious key Sid for every vehicle in the organization. The key is given as in condition 5.

$$Sid = (id, Q\mathcal{H}) \tag{5}$$

The produced key is appointed to the suitable vehicle after enrollment. The mysterious key for every client/vehicle is put away in the TA's key stockpiling dataset. All the while, the TA chooses an arbitrary whole number to appoint the private key for RSU. This irregular number is chosen as . Let $G1$ be an added substance cyclic gathering of request q produced by P. Subsequently, the RSU public key can be figured as in condition 6.

$$KRSU = \mathcal{R}RSUP \tag{6}$$

Here, RSU public key, generator P, hash work $\mathscr{k}$ and $G1$ will be distributed to all gadgets while the RSU private mystery key $\mathcal{R}RSU$ is kept mystery during this interaction. This cycle is utilized for enrolling the vehicle. Allow us to accept that the enrolled vehicle is entering the scope of RSU. Assuming that vehicle requests for any help from the VANET, key task is the vital undertaking. This vehicle v chooses a fractional private key as, and the comparing incomplete public key is given as in condition 7.

Where P is the generator, using these parameters service request, public key and vehicle id are delivered to the corresponding RSU which are arranged as $\langle ServiceRequest$, Qv, $id\rangle$. Once the partial public key Qv is generated, the RSU request to TA for providing the secret key S for vehicle id i.e. RSU request to TA for Sid. At this stage, we generate a secure hash function.

From here, the vehicle sends the authentication request as $\langle U, id, t, v\rangle$ and RSU performs the verification process whether $\alpha = \frac{\hat{F}(P,U)}{\hat{F}(Q_1,Q_{id})^v}$. (7)

In order to deliver the message, the following verification condition must be satisfied as in equation 8.

$$\frac{\hat{F}(P,U)}{\hat{F}(Q_1,Q_{id})^v} = \hat{F}(P, Q_{id}, \mathscr{R}_{RSU}) = \hat{F}(\mathscr{R}_{RSU}, P, Q_{id}) = \hat{F}(\mathscr{R}_{RSU}, Q_{id}) \tag{8}$$

After satisfying this condition, the authentication phase is completed.

IV. Data Encryption And Decryption

This stage presents the information encryption and unscrambling way to deal with give secure information trade. As per this cycle, the main assignment is to get the information utilizing encryption key which is utilized by recipient to scramble and unscramble the information by sender and beneficiary. This stage utilizes the state value ($state$) of recipient vehicle as an encryption key. To keep up with the area protection, this system utilizes hash state esteem prior to sending to the relating vehicle.

V. DIAGRAM

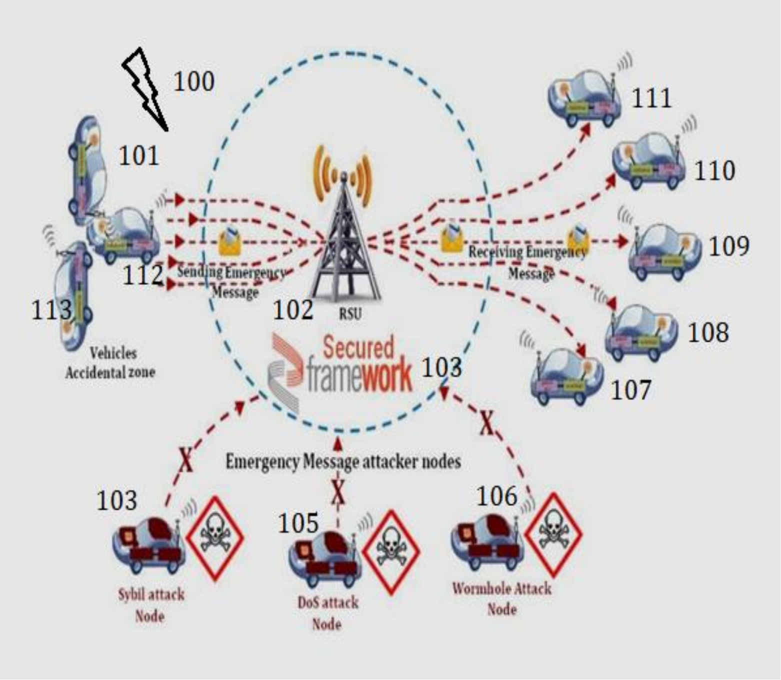

Fig. 1. Research scenario of VANET

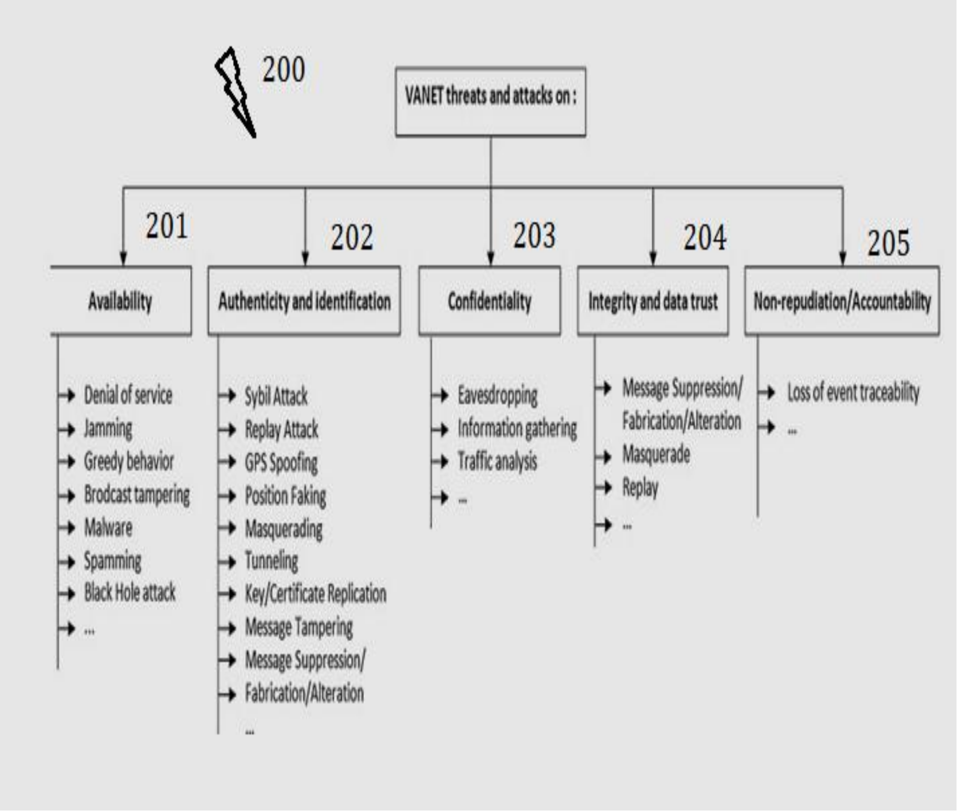

Fig 2. Examples of VANET threats and attacks

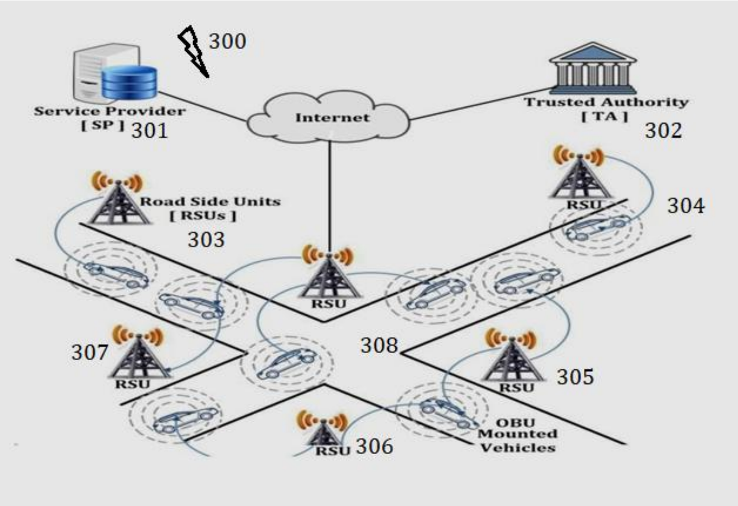
300
Service Provider [SP] 301
Internet
Trusted Authority [TA] 302
Road Side Units [RSUs] 303
RSU
304
RSU
307
RSU
308
RSU
305
OBU Mounted Vehicles
RSU 306

Fig 3: VANET Model

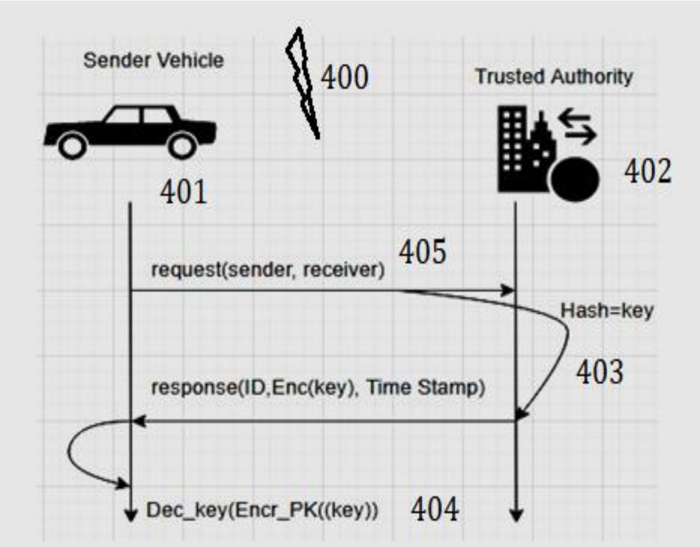

Fig 4: Data encryption process and key generation

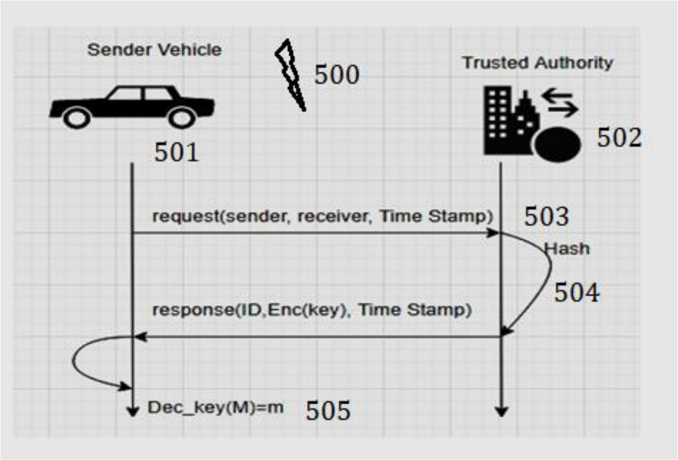
Sender Vehicle
500
Trusted Authority
501
502
request(sender, receiver, Time Stamp)
503
Hash
504
response(ID,Enc(key), Time Stamp)
Dec_key(M)=m
505

Fig 5. Data decryption process

VI. Description

This stage presents the information encryption and unscrambling way to deal with give secure information trade. As per this interaction, the main undertaking is to get the information utilizing encryption key which is utilized by recipient to encode and decode the information by sender and collector. This stage utilizes the state value ($state$) of beneficiary vehicle as an encryption key. To keep up with the area protection, this procedure utilizes hash state esteem prior to communicating to the relating vehicle.

These wellbeing messages ask for high security and low idleness. Then again, non-wellbeing applications incorporate traffic the executive’s undertakings and infotainment. Notwithstanding, infotainment applications don't need higher security. The wellbeing messages should be communicated rapidly and dependably. The powerful organization geography turns into a drawn-out task in VANET to convey the security message.

In spite of a few benefits of VANET in wellbeing and data application, these organizations require high security which is viewed as a difficult assignment.

- Vehicles trade privileged intel which can draw in aggressors to take and abuse the data henceforth, a solid security model is required.

- Due to high unique organization geography, no confirmation is performed because of this, the ill-conceived hubs take part in the Security is a superb worry because of following reasons: correspondence to hurt the VANET correspondence.

- The VANET design is framework less which is not difficult to assault by pariah aggressors henceforth giving security is imperative to the clients.

- Privacy safeguarding is a significant factor of VANET.

- Transmitting and getting precise data with next to no altering or mocking for secure correspondence.

- Data dependability, classification and client obscurity gives improved security to the organization.

Due to the previously mentioned reasons, VANET security is broadly contemplated. These assaults incorporate accessibility assaults like forswearing of administration (DoS) and dark opening connect, credibility assaults, for example, Sybil assault and GPS assault, information privacy, for example, listening in and information trust, non-disavowal like loss of occasion discernibility. Figure 2 shows a grouping of different assaults on VANET.

Likewise, cryptography based plans are additionally acquainted with secure the message. Acquainted cryptography approach with manage the Sybil assaults. A portion of the security plans are presented dependent on the key-administration convention, for example, introduced Diffie-

Hellman key age conspire. Key administration and key age are the significant phases of confirmation.

Introduced ID-based verification convention. Moreover, the cryptographic plans are extended dependent on the symmetric and deviated cryptography plans. Nonetheless, accomplishing security in these kinds of dynamic organizations is constantly viewed as a difficult assignment and different explores are as yet in progress to give greater security in VANETs. This work centers around on security necessities of VANET and presents a clever methodology for secure correspondence in VANETs. The fundamental commitments of the work are as per the following:

- Development of a clever methodology for bunch key circulation which incorporates confirmation interaction to further develop the organization security.

- Incorporating novel information encryption and decoding measure dependent on the Elliptic Curve Cryptography (ECC) conspire.

The remainder of the composition is coordinated as writing audit study, which is introduced in area 2. The proposed answer for the security and QoS upgrade in the VANET is introduced in segment 3 and segment 4 presents the test study. The relative investigation shows vigorous execution of the proposed model. At long last, segment 5 presents closing comments.

Preliminaries and Network Modelling

The VANET engineering contains a few parts like confided in power (TA), street side units (RSUs), specialist organization (SP), and installed unit (OBU) mounted vehicles and each substance of organization has appointed explicit assignments. For the most part, TA is considered as vehicle maker or transport the board division. Trust authority is liable for enrolling the RSUs and to create public and private keys to confirm every client. TA plays out a few calculations henceforth we accept that enough stockpiling is given to TA along sufficient calculation ability. Street Side Units (RSUs) are the foundations, which are sent at the street crossing point and street side which go about as transfers for V2I correspondence. Figure 3 shows required design of VANET for proposed framework.

The correspondence among RSU and vehicle is performed utilizing committed short-range interchanges (DSRC) convention. The fundamental assignment of RSU is to check the authenticity of the got message from vehicles. The specialist co-op gives various kinds of use to all vehicles. To give an application benefits, the RSU gets the message from vehicles, checks its authenticity and assuming the message is legitimate, sent to the application server for offering the necessary support. The SA, TA and RSU can impart through a security link channel. Also, OBU is a remote unit, which is introduced on the vehicle with GPS and a little gadget for short reach correspondences.

Security Requirements

In VAETs, data security and privacy are considered as an important factor to develop the secure VANET model. This work focuses on the following security requirements:

User authentication and message integrity: in this architecture, once the message is transmitted to the receiver, then the receiver must ensure the message integrity and validity by verifying the signatures.

Vehicle identity protection: the actual vehicle identity is only known by the trusted authority and the vehicles. This helps to maintain anonymity from other vehicles in the network.

Message traceability: during communication, if any bogus message is received by the receiver, then TA should be able to track the original identity of the vehicle.

Message stealing: during data communication of message transmission phase, the protocol should be able the secure the high confidentiality message by avoiding message stealing by attackers.

Fake Message attack: the fake messages are disseminated to harm the network entities hence the protocol should restrict the fake message circulation in the network.

Fake identity: according to this attack the real identity of vehicle is forged and used for concealing the information. Hence, the identity of vehicles should be anonymized to prevent this attack.

Similarly, here it focus on achieving the solution for non-repudiation attack, replay attack and DOS attack to develop a more robust and secure network architecture.

Hence, this work introduced a combined novel key management and data security approach for VANETs. The proposed model is implemented in two-fold manner where first of all key management is performed and later, data encryption is applied. The proposed approach is denoted as GKMC (Group Key Management & Cryptography Schemes).

TABLE I. ABBREVIATIONS

$\mathcal{G}_o, \mathcal{G}_N$	Additive cyclic group
$\mathscr{p}$	Large prime order for additive cyclic group
F	Bilinear map function
$\mathcal{R}RSU$	Random key for RSU
$KRSU$	Public key of RSU
$\mathbb{H}$	Hash function

VII. Results and Discussion

This segment shows the exploratory examination utilizing proposed approach. The got execution is contrasted and the current methods. This examination

Accomplished Security Issues

These proposed works accomplish the accompanying security issues, for example,

https://doi.org/10.17758/EIRAI18.F0523108

Validation: in this work, confirmation is a significant undertaking to keep away from the assailant hubs to join the organization. Afterward, Hash esteems are acquired from the key and a confirmation interaction is performed in the wake of accomplishing the RREP message from the imparting hub.

Message classification: this work applies symmetric cryptography where public and private discharge keys are created from the RSA key age strategy.

Area protection and secrecy: this security viewpoint is acquired by creating the Hash of the area of the vehicle and vehicle ID.

Execution Measurement Parameters

This segment presents the exploratory examination utilizing proposed approach. The presentation of proposed approach is estimated as far as bundle misfortune, throughput, and parcel conveyance, start to finish delay, normal message postponement and message misfortune proportion. The reenactment boundaries are given in table 2.

TABLE II. SIMULATION PARAMETERS

Simulation Parameter	Used Value
Simulation Area	1500m x1500m
Simulation Time	100s
Data Traffic	CBR
Route protocol	AODV
Mobility	Random Waypoint
Channel bandwidth	6 Mbps

As indicated by table 2, proposed approach is viewed as complete of 100 hubs which are sent in the 1500m x1500m region. The vehicles follow the Random Waypoint model with the consistent piece rate information traffic. All out 10 hubs are considered as broken hub which is liable for different assaults like Denial-of-administration, dark opening and knocking and so on In this work, we measure the presentation of proposed approach under different assaults to show the hearty exhibition. The got execution is estimated utilizing following execution measurements:

Parcel Loss Ratio: is estimated by taking the proportion of the dropped bundles which are created from the source yet not conveyed to the objective as in condition 9.

$$PLR = \frac{P_{Sent} - P_{received}}{P_{Sent}} \times 100 \qquad (9)$$

Where P_{Sent} denotes the number of sent data packets, $P_{received}$ denotes the received number of data packets.

Throughput: is measured by computing the total of bytes received successfully in one communication session. This is computed as in equation 10.

$$Throughput = \frac{P_{Sent} - P_{received}}{P_{Sent}} \times 100 \qquad (10)$$

Packet delivery ratio: this is measured by taking the ratio of delivered packet to the destination which are generated from source nodes. It can be calculated as in equation 11.

$$PDR = \frac{P_{received}}{P_{Sent}} \times 100 \qquad (11)$$

Average end-to-end delay: this is the time take by the data packet to reach to the destination. During this phase, the route discovery, data retransmission and propagation time etc. are considered. This is computed as in equation 12.

$$Delay = \frac{\sum_{i=1}^{P_{succes}} (D_i - s_i)}{P_{Succes}} \times 100 \qquad (12)$$

Where D_i denotes the i^{th} packet receiving time, s_i denotes the sending time for i^{th} packet and P_{succes} denotes the number of successfully transmitted packets.

Average message delay: this is the measurement of total delay occurred to deliver the message from one source to destination. This can be computed as in equation 13.

$$AverageDelay = \frac{\sum_{i}^{N_v} \sum_{m=1}^{M\_sent} \left(T_{sign}^{i\_m} + T_{trans}^{i\_m\_RSU} + T_{verify}^{i\_m\_RSU}\right)}{\sum_{i=1}^{N_v} M_{sent}^{i}} \qquad (13)$$

Where N_v is the total number of vehicles, $M_{sent}{}^{i}$ is the total number of packet sent by vehicle i,$T_{sign}^{i\_m}$ is the time required to sign a message by vehicle, $T_{trans}^{i\_m\_RSU}$ is the time require to transmit the message m to RSU and $T_{verify}{}^{i\_m\_RSU}$ is the time required for authentication. Similarly, we measure the message loss ratio as in equation 14.

$$Messagelossratio = \frac{\sum_{i=1}^{N_v} M_{sent}^{i} - \sum_{r=1}^{RSU^n} M_{rec}^{r}}{RSU^n * \sum_{i=1}^{N_v} M_{sent}^{i}} \qquad (14)$$

Comparative Performance Analysis

This section shows the comparative experimental analysis where, performance of the proposed approach is compared with the existing techniques by varying the number of vehicles, speed and malicious nodes in the network.

VIII. Result

1. Our Invention “Improved Security Mechanism for Emergency Messages of Vanet Cryptography Schemes. Vehicular Ad-hoc network (VANET) is one of the arising innovations for research local area to get different examination difficulties to build got system for independent vehicular correspondence. The great worry of this

https://doi.org/10.17758/EIRAI18.F0523108

innovation is to give proficient information correspondence among enrolled vehicle hubs. The few exploration thoughts are executed for all intents and purposes to work on by and large correspondence in VANETs by thinking about security and protection as significant parts of VANETs. A few instruments have been carried out utilizing cryptography calculations and strategies. In any case, these instruments give an answer just to some confined conditions and to restricted security dangers. Henceforth, the proposed novel system has been presented, executed and tried utilizing key administration method. It gives tied down network climate to VANET and its parts. Afterward, this component gives security to information bundles of crisis messages utilizing cryptography instrument. Henceforth, the proposed novel component is named Group Key Management and Cryptography Schemes (GKMC). The exploratory examination shows huge enhancements in the organization execution to give security and protection to crisis messages. This GKMC component will help the VANET clients to perform gotten crisis message correspondence in network climate.

2. According to claim1# the invention is to a "MAR SECURITY: IMPROVED SECURITY MECHANISM FOR EMERGENCY MESSAGES OF VANET USING GROUP KEY MANAGEMENT &CRYPTOGRAPHY SCHEMES (GKMC)" Vehicular Ad-hoc network (VANET) is one of the arising innovations for research local area to get different examination difficulties to build got system for independent vehicular correspondence.
3. According to claim1, 2# the invention is to a great worry of this innovation is to give proficient information correspondence among enrolled vehicle hubs. The few exploration thoughts are executed for all intents and purposes to work on by and large correspondence in VANETs by thinking about security and protection as significant parts of VANETs.
4. According to claim1, 2, 3# the invention is to a few instruments have been carried out utilizing cryptography calculations and strategies. In any case, these instruments give an answer just to some confined conditions and to restricted security dangers. Henceforth, the proposed novel system has been presented, executed and tried utilizing key administration method.
5. According to claim1,2,3,4# the invention is to a gives tied down network climate to VANET and its parts. Afterward, this component gives security to information bundles of crisis messages utilizing cryptography instrument. Henceforth, the proposed novel component is named Group Key Management and Cryptography Schemes (GKMC).
6. According to claim1, 2,3,4,5, # the invention is to a exploratory examination shows huge enhancements in the organization execution to give security and protection to crisis messages. This GKMC component will help the VANET clients to perform gotten crisis message correspondence in network climate.

IX. Acknowledgement

I would like to acknowledge Prof B.K Sarkar who helped me during the development of my research Paper. I express my sincere thanks to Prof. B.K Sarkar.

REFERENCES

[1] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162– 1182, 2021.
https://doi.org/10.1109/JPROC.2011.2132790

[2] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, H. Duan, and Q. Zeng, "Accessibility analysis and modeling for iov in an urban scene," IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4246–4256, 2020.
https://doi.org/10.1109/TVT.2020.2970553

[3] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "Sirc: A secure incentive scheme for reliable cooperative downloading in highway vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 6, pp. 1559–1574, 2022.

[4] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in vanets-an efficient and privacy-preserving cooperative downloading scheme," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1191–1204, 2020.
https://doi.org/10.1109/JSAC.2020.2986617

[5] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.
https://doi.org/10.1109/TITS.2015.2439292

[6] R. G. Engoulou, M. Bella¨ıche, S. Pierre, and A. Quintero, "Vanet security surveys," Computer Communications, vol. 44, pp. 1–13, 2014.
https://doi.org/10.1016/j.comcom.2014.02.020

[7] C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," IEEE Network, vol. 34, no. 2, pp. 37–45, 2020.
https://doi.org/10.1109/MNET.001.1900220

[8] Chhabra, Rishu, Seema Verma, and C. Rama Krishna. "A survey on driver behavior detection techniques for intelligent transportation systems." In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, pp. 36-41. IEEE, 2017.
https://doi.org/10.1109/CONFLUENCE.2017.7943120

[9] A. K. Agarwal, D. Ather, R. Astya, D. Parygin, A. Garg and D. Raj, "Analysis of Environmental Factors for Smart Farming: An Internet of Things Based Approach," 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART), 2021, pp. 210-214, doi: 10.1109/SMART52563.2021.9676305.
https://doi.org/10.1109/SMART52563.2021.9676305

[10] A. K. Agarwal, M. Anam, D. K. Sharma, R. Regin, M. Acharya and K. Ashok, "Application of Access Control Framework in Cloud Reliability," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 1-5, doi: 10.1109/ICOSEC51865.2021.9591973.
https://doi.org/10.1109/ICOSEC51865.2021.9591973

[11] A. K. Agarwal, R. G. Tiwari, R. K. Kaushal and N. Kumar, "A Systematic Analysis of Applications Of Blockchain in Healthcare," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 413-417, doi: 10.1109/ISPCC53510.2021.9609339.
https://doi.org/10.1109/ISPCC53510.2021.9609339

[12] R. G. Tiwari, A. K. Agarwal, R. K. Kaushal and N. Kumar, "Prophetic Analysis of Bitcoin price using Machine Learning Approaches," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 428-432, doi: 10.1109/ISPCC53510.2021.9609419.
https://doi.org/10.1109/ISPCC53510.2021.9609419

[13] Agarwal, A.K., Rani, L., Tiwari, R.G., Sharma, T., Sarangi, P.K. (2021). Honey Encryption: Fortification Beyond the Brute-Force Impediment. In: Manik, G., Kalia, S., Sahoo, S.K., Sharma, T.K., Verma, O.P. (eds) Advances in Mechanical Engineering. Lecture Notes in Mechanical

Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-16-0942-8_64
https://doi.org/10.1007/978-981-16-0942-8_64

[15] R. K. Jindal, A. K. Agarwal, and A. K. Sahoo, “Data analytics for analysing traffic accidents,” Test Eng. Manag., vol. 83, no. 14796, 2020.

[16] R. K. Jindal, A. K. Agarwal, and A. K. Sahoo, “Envisaging the road accidents using regression analysis,” Int. J. Adv. Sci. Technol., vol. 29, no. 5 Special Issue, pp. 1708–1716, 2020.

[17] T. Agrawal, A. K. Agrawal, and S. K. Singh, “Cloud sanctuary through effectual access control and cryptographic model,” J. Adv. Res. Dyn. Control Syst., vol. 11, no. 6, pp. 533–537, 2019.

[18] P. Kamat, A. Baliga, and W. Trappe, “An identity-based security framework for vanets,” in Proceedings of the 3rd international workshop on Vehicular ad hoc networks, 2006, pp. 94–95.
https://doi.org/10.1145/1161064.1161083

Pitty Nagarjuna (Author)

At present he is working as a Principal Research Scientist, Indian Institute of Science, Bengaluru, India. He was also published book chapters, research papers and presented in various conferences in the subject of computer science, information science and management at national and international level. Besides that actively participated a conference chair at various national & international conferences. He’s qualification PhD pursuing at REVA University, Bengaluru, Obtained Master of Engineering (Computer Science & Engineering) from Satyabhama University, Chennai, India. Master of Science (Information Systems & Management) from the department of Management studies at Sri Venkateswara University, Tirupati, India and Bachelor of Technology (Computer Science & Engineering) from Acharya Nagarjuna University, Guntur, India.