Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach

Satya Sandeep Kanumalli[1]
Research Scholar, CSE Department
University College of Engineering
Acharya Nagarjuna University.and Asst.Professor
Vignan's Nirula Institute of Technology and Science for Women, Guntur 522009
India

Anuradha Ch[2]
CSE Department, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada 52007, India

Dr. Patanala Sri Rama Chandra Murty[3]
CSE Department, Acharya Nagarjuna University
Guntur 522510, India

***Abstract*—We live in the world of "Internet of Everything", which lead to advent of different applications and Internet of vehicles (IOV) of one among them, which is a major step forward for the future of transportation system. Vehicle to vehicle (V2V) communication plays a major role in which a vehicle may send sensitive, non-sensitive messages and these messages are encrypted with public keys, which makes distribution of public keys is a major problem due to the vehicle need to be anonymous having pseudonyms which changes more frequently and makes it more complicated. Here we proposed a hybrid approach, which uses existing Public key certificate for authorization of the vehicle and Identity Based Encryption to generate public keys from the pseudonyms and use it in secure V2V communication without compromising anonymity of the vehicle.**

Keywords*—Privacy; internet of vehicles; hashing; IBE; public key certificate

I. INTRODUCTION

Due to advent of wireless communication and internet there are many things that are connected and communicate with each other with out the intervision of human and many applications are derived in which Internet of vehicles (IOV) stands tall as its is big thing which enables autonomous driving which changes the future of transportation [1][3].

IOV[17][18] is derived from age old VANETS in which the vehicles and its infrastructure are interconnected using internet technologies like 4G and 5G, but the most of the arcitecture remains the same as the treditional VANETs, which inherets some of the challenges like security and privicy of the vehicle and comminication as well.

Thre are different types of communication players Like Vehicle, RSU, CA etc and they can enable different types of communication like V2V, V2R etc and can also extand as V2X which enables the communication between the vehicle and pedestrian, smart objects etc. out of which V2V communication playes amajor role through the vehicle exchanges different types of messages like safety and non safety messages[15]. V2V communication playes amajor role in the whole IOV communication, through the vehicle exchanges different types of messages like safety and non safety messages, when it comes to sefity messages time is very critical and for non safety message time may not be critical[21].

V2V messages should be secured and yet not compramising the privicy of the vehicle, as vehicles uses masking identites called Pseudonyms. A vehicle communicates 100's of messages every ms and they are different forms of attacks an attacker may plan like attacks [10] on privacy compromising the location and the real identity of the vehicle of the vehicle, attacks on integrity of the message in which the attacker may modify the message, eavesdropping through which the attacker tries to read the communication, different solutions are been proposed to combat security problems in V2V communication, which are broadly classified in to three types.

a) Hardware based solutions in which the attacks are identified at the physical level[25][26] by utilizing channelization and using provability distribution functions in which these solutions only work with the attacks on physical layer and completely ignore the attacks on higher layers

b) IBE based solutions in which different solutions utilizes a trusted authority[8][9], which distributes the keys to the vehicles and some of the solutions utilizes certificates and some may not very time the trusted authority [16] must act as a middle man which incurs delay and bottle neck in the network. Some completely ignore the usage of pseudonyms, which compromises the privacy of vehicle.

c) The other solutions are based on trust-based mechanisms[22][23][24], in which every vehicle is associated with a trust value and may vary depending on vehicle behavior [19] and there also exist a trusted third party (TTP) or mutual group trust management, which evaluates and isolates the attacker depending on its trust value[27]. These solutions may not work all the time as the attacker may act normal to improve its trust value and the TTP may compromise.

In this paper we address the problem using a hybrid mechanism which utilizes the existing public key certificate and Identity Based Encryption (IBE) by which the vehicle can use pseudonyms and hide its identity and yet traceable by the Transport Authorities which can revoke the certificate in case of suspicious vehicle [28].

The rest of the paper organized as follows; in Section II we briefly discuss the existing approaches along with its drawbacks, in Section III we have presented the System Architecture we followed, in Section IV we thoroughly discussed our hybrid approach and also we presented the proof of work for IBE, in Section V we presented the threat model with the adversary and its different forms of attacks, in Section VI shows our simulation results, in Section VII presents conclusion and future work.

II. Related Work

Works related to physical layer security focus on physical aspects. Hanet al. [1],based on securing sub carrier allocation where the eavesdropper may intercept the communication, so the sub carrier allocation, joint rally selection is done by using the provability calculated by forming RGB, Random by parity Graph which given a good results as the work is based on physical layer security, where most of the attacks are undertaken on higher layers.

Jinyuan Sun et al. [20] Based on IBE which uses threshold based secret sharing and using pseudonyms for preserving privacy here RTA acts as middle man which generates the keys and it is susceptible to sing point of failure which make the whole system prone to DOS attack.

Liu, Yanbing et al. [3] have proposed an authentication and key agreement scheme for safeguarding V2V communication which involves third party Trusted authority in the communication which incurs delay as every time TA is also a part of authentication.

Debiao He et al. [4] proposed a scheme based on IBE which does not use Bilinear pairings, called CCPA conditional Privacy Preserving Authentication scheme which is better proved to reduce the computational cost which again shows the trusted authority plays a key role which ultimately be a single point of failure and the communication is made through internet which can be a bottle neck in the communication.

Song, Jun et al. [5] have proposed a IBE scheme, which is light weight and doesn't use certificates for authentication and RTA generates the master key and it also manages the communication without RSU, without public key certificates after fraud detection revocation is an issue.

T.W. Chim et al.[6] have proposed a privacy preservation schemes for unicast and group communication in which RSU stands as a middle man, which verifies the signatures which shows the reduction of message overhead, but it incurs load on RSU, and it may prone to Sybil attack.

Lee et al. [7] have proposed a batch message verification scheme based on bilinear pairing, message singing and verification process, is a bit complicated which incurs overhead in communication.

III. System Architecture

IOV has no standardized architecture defined, different types of architecture's proposed cloud based, fog and cloud hybrid architecture and these derived from basic VANET architecture.

Here we follow very basic IOV architecture shown in Fig. 1, which consists of vehicles V, equipped with Dedicated Short range communication DSRC [11]boards, these boards are fixed as a Tamper proof Device TPD [12], and these are called on board units OBU. DSRC is the modified form of standardWi-Fi called 802.11p [29], which uses 5.9 GHz band and the layers of 1609, which together called WAVE.

Roads, parking lots and other places in which a car can move are covered by Road Side Units (RSU), generally these are equipped with high computational power processors and wired and wireless technologies [30] like 4G, 5G, WAVE etc. RSUs are aligned in such a way that they are in a line of site to one another,for local and global handover management, and they are interconnected with RSU controller RSUC which acts as switching station and it also moves the data from TA and CA back and fourth.

As shown in Fig. 1 Transport Authority TA is the root of the system, which registers the vehicles soon after it is been purchased from the show room and it creates an entry in its database, which contains all the vehicle information, as well as driver information and other license data.

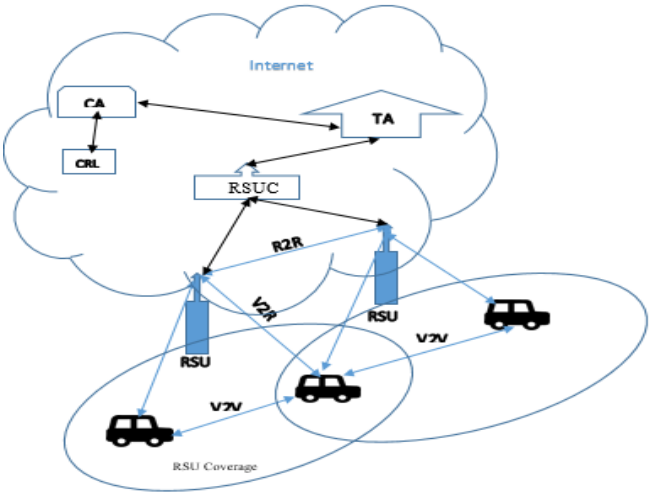

Fig. 1. IOV System Architecture.

Certification Authority CA Creates a Public key certificate for every vehicle after registration with TA, which contains public key information [31] along with the expiry and this information, can be accessible to RAUs as well and CA has a database CRL certificate revocation list [32] which can be used by RSU to send revocation request for vehicles found to be attackers[33].

IV. Proposed IBE-PKI based Hybrid Approach

The proposed system is based on bilinear maps on abelian groups based on [2][21], which maps the elements from two Additive groups G_1, G_2 to a target group G_T, here we follow a hybrid approach rather than pure IBE in which every vehicle should process the public key certificate issued by CA and on the top of it uses IBE to avoid the delay caused by certificate verification every time. The terminologies used in the manuscript are represented in Table I.

TABLE. I. TERMINOLOGIES USED

Abbreviation	Full form or meaning
V	Vehicle
V_A	Adversary
OBU	On board unit
TPD	Tamper Proof Device
WAVE	Wireless Access in Vehicular Networks
DSRC	Dedicated Short Range Communication
RSU	Road Side Units
V2V	Communication between vehicles
V2R	Communication between vehicle and RSU
R2R	Communication between RSUs
RSUC	RSU controller
TA	Transport Authority
CA	Certification Authority
CRL	Certificate revocation List
KCG	Key Generation Center
P	Prime Number
G, G_T	Generator and target Groups
MS_R	RSUs Master Secret
e	Bilinear map
H_1	Hash function maps $[0,1]^l$ -> G
H_2	Hash function maps G-> $[0,1]^l$
P_{id}	Pseudonym Identity
SK_{id}	Secret generated to P_{id}
M_{v2}	Message for Vehicle V_1 from V_2 in plain text
CT_{V2}	Cipher text generated for M_{v2}
$\|\|$	Concatenation
$\oplus$	XOR operation
r	Random number in Z_p
Q	g^{α}

The proposed method can be viewed in five stages: i) Vehicle registration with Certification Authority is, ii) RSU Setup, iii) Vehicle registration with RSU, iv) Encryption by vehicle V_2, v) Decryption by Vehicle V_1 and some of these steps are carried only once in the communication scenario.

1) Vehicle registration with certification authority: Vehicle V soon after its onboard unit (OBU) is configured, public, private key pairs PUV, PRV are generated and sent along with its vehicle details, and unique identifier to Certification Authority (CA) for its public key certificate, CA verifies the details as shown in Fig. 2, store them to its database and issues the vehicle with its public key certificate CV. This step is carried only once in the vehicles lifetime unless the hardware gets changed or the Certificate is expired.

2) RSU setup: RSU are assumed to be with in the line of sight to one another and every time a vehicle moves from one RSU to another RSU, every RSU configures itself and generates master secret on hourly or daily basis.

a) RSU acts as Key Generation Center (KGC), it chooses a master secret MS_R and identifies global parameters perm (P, G, G_T, g, e)

P is a prime number

G, G_T are two cyclic groups generator and target, one additive and one multiplicative groups

g is the generator of G

e is the bilinear map element from G -> G_T

b) perm can also be given as (P, Q, H_1, H_2)

Where H_1 and H_2 are the hash functions

H_1 maps a string or id of the vehicle to element in G

$H_1 = [0,1]^l$ -> G

H_2 maps element in G_T back to the string

H_2 = G -> $[0,1]^l$

$MS_R = \alpha$

3) Vehicle registration with RSU: Vehicle holds the public key certificate, as it should not disclose its identity to the other vehicles it should not publically announce its certificate instead it gains pseudonyms by showing certificate to RSU as shown in Fig. 3. These pseudonyms can be changed when required or following pattern or randomly making the vehicle anonymous.

a) Vehicle V1 when it enters new RSU region, sends its public key certificate to RSU, RSU verifies the certificate and its period of validity and issues a set of pseudonyms (P_{id1}, P_{id2}, …P_{idn})$_{V1}$ which can be utilized for communication.

b) Vehicle V1 when it intends to change its pseudonym, it sends its new P_{id} to RSU, RSU generates secret key SK_{id} by applying H1 as follows and its master secret key α.

$SK_{id} = (H_1(P_{id}))^{\alpha}$

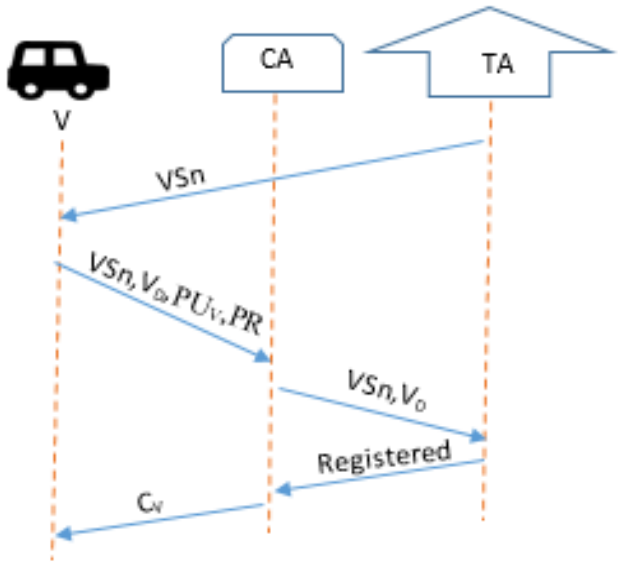

Fig. 2. Vehicle Registration with CA.

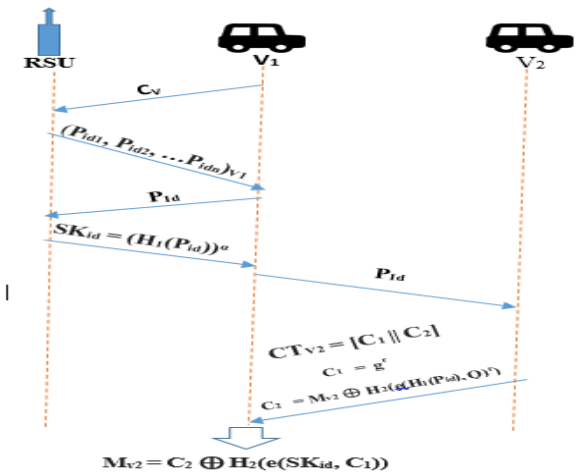

Fig. 3. Message Encryption and Decryption.

The above step maps the pseudonym which is string of $[0,1]^l$ to element in G^{α}

4) Encryption by vehicle V_2: When a vehicle tries to send a message may be Basic safety or emergency Broad Cast messages some of the messages needs encryption in certain cases and these messages must be confidential and as well as the system must preserve integrity so encryption is the only means.

a) If a vehicle V_2 wants to send a confidential message to vehicle V_1, V_2 prepares the message M_{v2} which is also a string of $[0,1]^l$.

b) It have its global parameters which is acquired from RSU (P, g, Q, H_1, H_2).

$Q = g^{\alpha}$

c) V_2 encrypts the message using pseudonymP_{id} of vehicle V_1, which produces the cypher text as follows.

$CT_{V2} = [C_1 \| C_2]$

$C_1 = g^r$

r is the random number in Z_p

$$C_2 = M_{v2} \oplus H_2(e(H_1(P_{id}), Q)^r) \quad (1)$$

d) Vehicle V_2 sends cipher text CT_{V2} to V_1

5) Decryption by Vehicle V_1

a) Vehicle V_2 soon after it receives CT_{V2} from V_2 it decrypt the message using its secret key SK_{id} as follows

$$M_{v2} = C_2 \oplus H_2(e(SK_{id}, C_1)) \quad (2)$$

b) Proof of correctness

$M_{v2} = C_2 \oplus H_2(e(SK_{id}, C_1))$

Substituting C_2 from eq(1) in eq(2)

$$= M_{v2} \oplus H_2(e(H_1(P_{id}), Q)^r) \oplus H_2(e(SK_{id}, C_1)) \quad (3)$$

Substituting SK_{id}, C_1 in eq (3)

$= M_{v2} \oplus H_2(e(H_1(P_{id}), Q)^r) \oplus H_2(e((H_1(P_{id}))^{\alpha}, g^r))$

Substituting Q in above equation

$= M_{v2} \oplus H_2(e(H_1(P_{id}), g^{\alpha})^r) \oplus H_2(e((H_1(P_{id}))^{\alpha}, g^r))$

$= M_{v2} \oplus H_2(e(H_1(P_{id}), g))^{\alpha r} \oplus H_2(e((H_1(P_{id})), g))^{\alpha r}$

$= M_{v2}$

V. Threat Model

Here we assume a Adversary which is planted at every RSU and it is having all the computation and communication technology, which also act as any other vehicle but the main job is to intercept the traffic, modify the messages, track the vehicles to map the original identities.

a) Attacks on confidentiality: When vehicle V_2 wants to send a message M to V_1, it encrypts the message and sends $CT_{V2} = [C_1 \| C_2]$ to V_1 and the adversary V_A tries to decrypt the message and to extract r out of C_1 is a complex and computing SK_{id} from the known P_{id} is a discrete logarithmic problem which V_A is incapable of computing.

b) Attacks on integrity: Vehicle V_2 sends cipher text in the form $[C_1 \| C_2]$ to V_1 and before it reaches V_1, Adversary V_A captures the message and tries to modify the message by preparing M_{v2} and prepare $C_2^{\wedge} = M_{v2} \oplus H_2(e(H_1(P_{id}), Q)^r)$ by choosing a random $r^{\wedge}$ and precomputing $C_1^{\wedge} = g^{r^{\wedge}}$ and sends $[C_1^{\wedge} \| C_2^{\wedge}]$ to V_1,.

V_1 computes $M_{v2}^{\wedge} = C_2^{\wedge} \oplus H_2(e(SK_{id}, C_1^{\wedge}))$

Decryption was a success and V_1takes the message as granted, to overcome this problem V_2 must also concatenate an encrypted hash along with the cipher text.

$CT_{V2} = [C_1 \| C_2 \| EH(M_{V2})]$

$EH(M_{V2})$ is the encrypted hash of M_{V2} with P_{id} of V_1 so that only V_1 can decrypt the hash and can check for integrity. As V_A can only tamper Message but not hash integrity of the message is preserved.

c) Attacks on anonymity: Anonymity should be preserved in IOV as the adversary can track the vehicle and understand its driving pattern, behavioral patterns, and may employee some physical attacks like kidnap, Murder, extortion, etc. For the adversary VA to get the real identity of the vehicle Vid it must get the certificate CV1 knowing Pid, only RSU is having the data associated with CV1 and we assume RSU to be a tamper proof device. It is impossible to the adversary.

As the pseudonyms keeps changing very time and the vehicle acquires new pseudonyms under new RSU and it is computationally infeasible to track the original identity of the vehicle from Pseudonyms.

VI. Simulation Results

A. Simulation Setup

For Simulation we make use of of a highway Junction road map at Guntur using open street map (OSM) and imported the map to SUMO [13] traffic simulator. We have created traffic nodes and other boundaries using polyconvert and netconvert commands contained in the SUMO 0.25.0, we have used randomTrips.py to create random trips for the vehicles with different intervals with variable arrival rates say

1, 1.2, 2, 2.5 vehicles every second each vehicle arrive into the map and depart at variable rates and we setup the speed range to a max of 60 kmph.

For network simulation, we use OMNET++ 5 [14], having Venius Package, which enables the network simulation for SUMO traffic having RSU and the nodes enabled with DSRC stacks, and we have created different communication scenarios with incremental number of vehicles and variable no of attackers, the attackers as discussed in the threat model have the same capabilities as the Vehicle node. These attackers are intentionally implanted in to the network at different points, and have two basic functionalities. Some of them defined to be in the radio coverage of a vehicle and listen to the traffic between RSU and Vehicle node, store the pseudonyms and try to track the vehicle even pseudonym keeps changing and the other are defined to eavesdropping the communication between the vehicles and try to decrypt the messages.

B. Performance Evaluation

Here we consider three scenarios in which we evaluate the performance of the system one is the 'idle–IOV' which evaluates the idle condition with no attackers and no security mechanism implemented, one called 'attack-IOV' in which we implant attackers and with no security mechanism implemented and the other is our proposed IBE-PKI based Hybrid approach called 'IPH-IOV', in which we implement our defense mechanism along with the attackers implanted.

C. Computational Overhead

It is the extra work done by the CPU to execute the whole scenario and it is calculated by summing up the CPU cycles consumed by all the nodes in the network.

Here on the x-axis, we plot the No. of vehicles varies from 0 to 250 and on Y-axis we took computational overhead % varies from 0 to 1 and Fig. 4 shows computational overhead in Idle-IOV is very low as there is no much additional computation done by the vehicles or by the system, In our proposed IBE-PKI the computational overhead is initially not much high but as the number of vehicles increases in the system, the number of computations also increases due to the key computations and exchanges in the system and the Attack-IOV is between Idle-IOV and IBE-PKI as the computation is not much needed and the attackers computation makes it deviated from the Idle-IOV.

D. End to End Delay

It is the total delay imposed on the packet from sender to the receiver and End-to-End delay is given as follows.

End to End Delay = Σ (packet arrival time – Packet send time) / Σ (No. of connections).

On x- axis, we plot the simulation time that varies from 10 to 50 sec and on y-axis, we plot End to End Delay in mille seconds, varying from 0 to 700 ms. Fig. 5 shows End to End delay of the Idle-IOV is very low compared to other two as there are no attackers in the system no packets are delayed and it increases with simulation time, on the other hand Attack-IOV have high End to End delay in the system due to the attackers delay or drop the packets.

Our IBE-PKI have shown some delay compared to Idle-IOV due to key generation, encryption and decryption, it lies very close to Idle-IOV and it gave a good result compared to Attack-IOV which is much higher.

E. Packet Delivery Ratio

It is the ratio of the packets sent and received

Packet Delivery ratio = Σ No. of packets send / Σ No. of packets received

On x- axis, we plot the No. of vehicles that varies from 40 to 200 and on y-axis we plot End to End Delay % that varies from 0 to 2.

Fig. 6 shows Packet Delivery Ratio of the Idle-IOV is very high compared to other two as there are no attackers in the system no packets are delayed or dropped and it increases with the increase in number of vehicles, on the other hand Attack-IOV have low Packet Delivery Ratio in the system due to the attackers delay or drop the packets which ultimately decreases Packet Delivery Ratio.

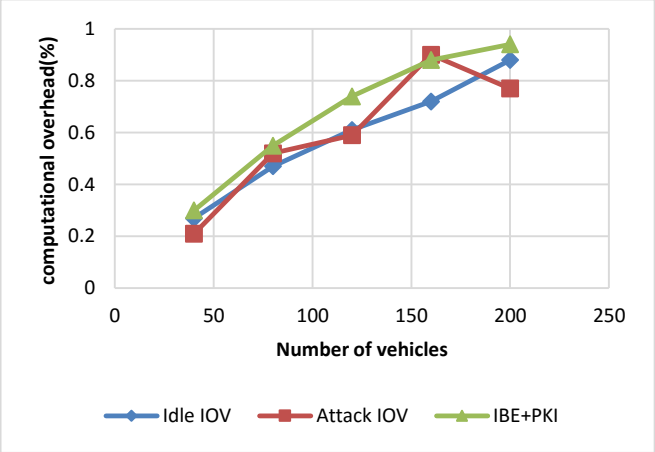

Fig. 4. Computational Overhead.

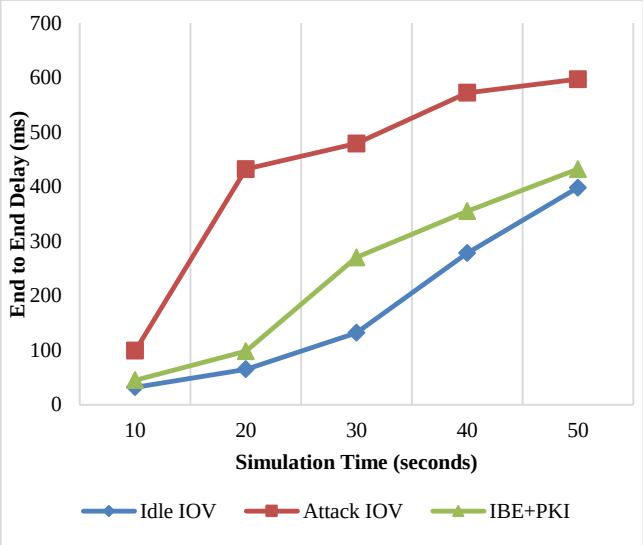

Fig. 5. End-to-End Delay.

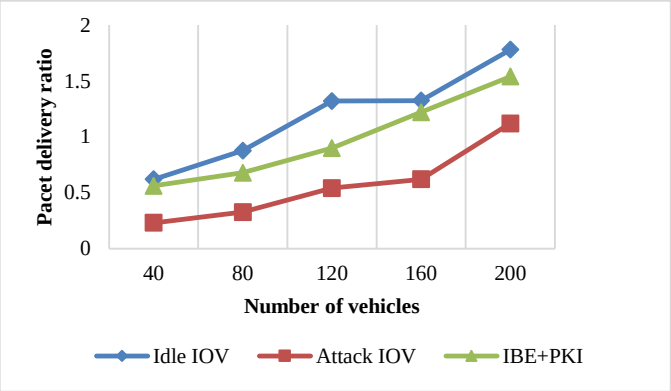

Fig. 6. Packet Delivery Ratio.

Our IBE-PKI have shown a very good result compared to Attack-IOV as it reduces the delay or drop of packets caused by the attackers and the results are very close to Idle-IOV.

F. Network Throughput

It is the sum of the packets delivered to the receivers successfully. Throughput is depicted in Fig. 7.

Throughput = Σ No. of packets received

On x- axis we plot the number of vehicle that varies from 40 to 200 and on y-axis, we plot Throughput in Megabits/ sec, varying from 0 to 1400 Mbps. Fig. 6 shows Network Throughput of the Idle-IOV is very high compared to other two as there are no attackers in the system no packets are delayed or dropped and it increases with the increase in number of vehicles, on the other hand Attack-IOV have low Network Throughput in the system due to the attackers delay or drop the packets which ultimately effects the Network Throughput value. Our IBE-PKI have shown a very good result compared to Attack-IOV as it reduces the delay or drop of packets caused by the attackers which increases the Network Throughput and the results are very close to Idle-IOV.

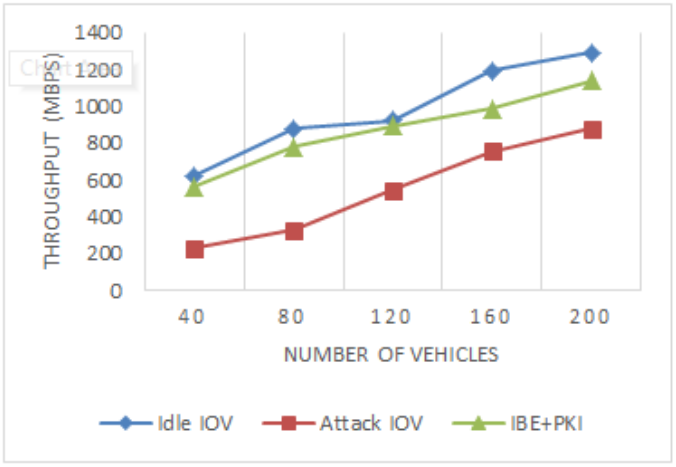

Fig. 7. Network Throughput.

VII. Conclusion and Future Work

Our Hybrid framework have safeguarded the system from the attackers yet not compromising the privacy of the vehicles and having significantly less computational delay and gave a good results compared to the other systems and the results obtained are close to the idle scenario. As a future work we try to still reduce the computational delay and also test the proposed mechanism in the real-world.

References

[1] Han, Di, Bo Bai, and Wei Chen. "Secure V2V communications via relays: Resource allocation and performance analysis." IEEE Wireless Communications Letters 6.3 (2017): 342-345.

[2] Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." Annual international cryptology conference. Springer, Berlin, Heidelberg, 2001.

[3] Liu, Yanbing, 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 18.10 (2017): 2740-2749.

[4] He, Debiao, et al. "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks." IEEE Transactions on Information Forensics and Security 10.12 (2015): 2681-2691.

[5] Song, Jun, et al. "Toward an RSU-unavailable lightweight certificate less key agreement scheme for VANETs." China Communications 11.9 (2014): 93-103.

[6] Chim, Tat Wing, et al. "SPECS: Secure and privacy enhancing communications schemes for VANETs." Ad Hoc Networks 9.2 (2011): 189-203.

[7] Lee, Cheng-Chi, and Yan-Ming Lai. "Toward a secure batch verification with group testing for VANET." Wireless networks 19.6 (2013): 1441-1449.

[8] S. Tangade, and S. S. Manvi, "Scalable and privacy-preserving authentication protocol for secure vehicular communications," in Proc. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017, pp. 1-6.

[9] Cui, Hui, Robert H. Deng, and Guilin Wang. "An Attribute-Based Framework for Secure Communications in Vehicular Ad Hoc Networks." IEEE/ACM Transactions on Networking(2019).

[10] Azees, Maria, Pandi Vijayakumar, and Lazarus Jegatha Deborah. "Comprehensive survey on security services in vehicular ad-hoc networks." IET Intelligent Transport Systems10.6 (2016): 379-388.

[11] Kenney, John B. "Dedicated short-range communications (DSRC) standards in the United States." Proceedings of the IEEE 99.7 (2011): 1162-1182.

[12] Mir, Zeeshan Hameed, and Fethi Filali. "LTE and IEEE 802.11 p for vehicular networking: a performance evaluation." EURASIP Journal on Wireless Communications and Networking 2014.1 (2014): 89.

[13] Krajzewicz, Daniel, et al. "SUMO (Simulation of Urban MObility)-an open-source traffic simulation." Proceedings of the 4th middle East Symposium on Simulation and Modelling (MESM20002). 2002.

[14] Varga, Andras. "OMNeT++." Modeling and tools for network simulation. Springer, Berlin, Heidelberg, 2010. 35-59.

[15] Kanumalli, Satya Sandeep, Anuradha Ch, and Patanala Sri Rama Chandra Murty. "Advances in Modelling and Analysis B." Journal homepage:http://iieta.org/Journals/AMA/AMA_B 61.1 (2018): 5-8.

[16] Kanumalli, Satya Sandeep, Anuradha Chinta, and Patanala Sri Rama Chandra Murty. "Isolation of Wormhole Attackers in IOV Using WPWP Packet Isolation of Wormhole Attackers in IOV Using WPWP Packet."

[17] Gerla, Mario, et al. "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds." 2014 IEEE world forum on internet of things (WF-IoT). IEEE, 2014.

[18] Alam, Kazi Masudul, Mukesh Saini, and Abdulmotaleb El Saddik. "Toward social internet of vehicles: Concept, architecture, and applications." IEEE access 3 (2015): 343-357.

[19] Kanumalli, Satya Sandeep, Anuradha Ch, and Patanala Sri Rama Chandra Murty. "Advances in Modelling and Analysis B." Journal homepage:http://iieta.org/Journals/AMA/AMA_B 61.1 (2018): 5-8.

[20] Sun, Jinyuan, et al. "An identity-based security system for user privacy in vehicular ad hoc networks." IEEE Transactions on Parallel and Distributed Systems 21.9 (2010): 1227-1239.

[21] Lakshman Narayana Vejendla and Bharathi C R ,(2018),"Multi-mode Routing Algorithm with Cryptographic Techniques and Reduction of Packet Drop using 2ACK scheme in MANETs", Smart Intelligent Computing and Applications, Vo1.1, pp.649-658.DOI: 10.1007/978-981-13-1921-1_63.

[22] Lakshman Narayana Vejendla and Bharathi C R, (2018), "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS", Modelling, Measurement and Control A, Vol.91, Issue.2, pp.73-76.DOI: 10.18280/mmc_a.910207.

[23] Lakshman Narayana Vejendla , A Peda Gopi and N.Ashok Kumar,(2018)," Different techniques for hiding the text information using text steganography techniques: A survey", Ingénierie des Systèmes d'Information, Vol.23, Issue.6,pp.115-125. DOI: 10.3166/ISI.23.6.115-125.

[24] A Peda Gopi and Lakshman Narayana Vejendla (2018), "Dynamic load balancing for client server assignment in distributed system using genetic algorithm", Ingénierie des Systèmes d'Information, Vol.23, Issue.6, pp.87-98.DOI: 10.3166/ISI.23.6.87-98.

[25] Lakshman Narayana Vejendla and Bharathi C R,(2017),"Using customized Active Resource Routing and Tenable Association using Licentious Method Algorithm for secured mobile ad hoc network Management", Advances in Modeling and Analysis B, Vol.60, Issue.1, pp.270-282. DOI: 10.18280/ama_b.600117.

[26] Lakshman Narayana Vejendla and Bharathi C R,(2017),"Identity Based Cryptography for Mobile ad hoc Networks", Journal of Theoretical and Applied Information Technology, Vol.95, Issue.5, pp.1173-1181. EID: 2-s2.0-85015373447.

[27] Lakshman Narayana Vejendla and A Peda Gopi, (2017)," Visual cryptography for gray scale images with enhanced security mechanisms", Traitement du Signal,Vol.35, No.3-4,pp.197-208. DOI: 10.3166/ts.34.197-208.

[28] A Peda Gopi and Lakshman Narayana Vejendla, (2017)," Protected strength approach for image steganography", Traitement du Signal, Vol.35, No.3-4,pp.175-181. DOI: 10.3166/TS.34.175-181.

[29] Lakshman Narayana Vejendla and Bharathi C R,(2016),"Secured Key Production and Circulation in Mobile Ad hoc Networks Using Identity Based Cryptography", International conference on Engineering and Technology, Vol.1, pp.202-206.

[30] A Peda Gopi and Lakshman Narayana Vejendla, (2019)," Certified Node Frequency in Social Network Using Parallel Diffusion Methods", Ingénierie des Systèmes d' Information, Vol. 24,No. 1, 2019,pp.113-117..DOI: 10.18280/isi.240117.

[31] Lakshman Narayana Vejendla and A Peda Gopi, (2019)," Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology", Revue d'Intelligence Artificielle , Vol. 33,No. 1, 2019,pp.45-48.

[32] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM journal on computing 32.3 (2003): 586-615.

[33] Hu, Hao, et al. "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET." IEEE Transactions on Vehicular Technology 66.2 (2016): 1786-1797.