ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

A Secure and Efficient Vehicle Communication Scheme Using FP Tree Algorithm in Vehicular Ad Hoc Network

Punam R.Sathe[1], Ganesh N.Dhanokar.[2]

M. E Student, Department of Computer, G.H.Raisoni College of Engineering, Jalgaon,

North Maharashtra University India[1]

Department of Information Technology, G.H.Raisoni College of Engineering, Jalgaon,

North Maharashtra University India[2]

ABSTRACT: Ordinarily, authentication in vehicular ad-hoc networks (VANETs) customs Public Key Infrastructure (PKI) to verify the truth of messages and the identity of message senders. The issues considered in the authentication schemes include the level of security and computational efficiency in verification processes. However, these schemes may not work well in VANET scenarios. For instance, it is difficult for a Roadside Unit (RSU) to verify each vehicle's signature sequentially when a large number of vehicles emerge in the coverage areas of an RSU. In proposed system we prefer Frequent Pattern Tree Algorithm for communication In VANET, algorithm is less time consuming. Mostly proposed schemes focus on guarantee the security and privacy of VANET information**.**

KEYWORDS:Message Authentication;Proxy Vehicle;Vehicular adhoc network(VANET).

I. INTRODUCTION

VANET (Vehicular Ad-hoc Network) may be a form of Eduard MANET (Mobile Ad-hoc Network), that may be a next-generation networking technology that has communication between vehicles or between a vehicle associate decreed an RSU (Road aspect Unit) victimization wireless communication. Transport ad-hoc networks (VANETs) have attracted intensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs include entities together with On-Board Units (OBUs) infrastructure Road-Side Units (RSUs). Since vehicles communicate through wireless channels, a range of attacks like injecting false data, modifying and replaying the disseminated messages may be simply launched. A security attack on VANETs will have severe harmful or fatal consequences to legitimate users. Consequently, making certain secure transport communications may be a should before any VANET application may be place into apply.

II. RELATED WORK

An Expedite Message Authentication Protocol (EMAP) for VANETs, which exchanges the inefficient CRL check technique by an effective revocation checking process. Single-hop broadcast, multiple forwarding of packets, store the message in different RSU areas[14].

EMAP customs a profligate HMAC function and novel key circulation scheme paying probabilistic arbitrary key supply [1]. Based on decentralized CA, 2FLIP only needs numerous dangerous lightweight hashing methods and a fast MAC action for message signing and verification among vehicles [2].EMAP can reduction the message damage percentage due to the message confirmation interruption associated with the predictable authentication approaches using CRL[3]. In addition, the RSU is able to autonomously prove the outputs since the verification function of the proxy vehicles [4]. To check the message validity at RSU, a batch verification of all signed messages is being performed by RSU, which is known as Identity-based batch verification (IBV)[5]. ID based signature scheme which consists of four algorithms namely setup, extract, sign and verify [6]. The other vehicles can also make the message

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

authentication and identity verification based on the techniques of chameleon hash, HMAC and Diffie-Hellman key exchange [13].

III. PROPOSED ALGORITHM

1 Trusted Authority:

- All works are simply distributed by Trusted Authority.
- Dynamic Keys are distributed by TA to all vehicles.
- Trace the both Identity (real, hateful) of Vehicle.

2 Dynamic Keys:

- 32 bit Dynamic keys.
- Assign to the vehicle.
- All vehicles having unique key.

3 Node (vehicle) link:

- Node is link with each other.
- Select the shortest path logically.

4 Attach Path:

- Physical path established.
- Path is ready to send the data.

5 Proxy Vehicle:

- Verify signature of vehicle
- After verification process data will be forwarded to RSU.
- Proxy vehicles which achieves batch authentication of communication and sends the outcome to RSU[22].

6 Road Side Units

- Accept data from proxy vehicle.
- All verified data will be forward to the trusted authority.

a) System parameter generation:

- The TA stores UV = {RIDi|1 ≤ i ≤ n}. RIDi = Real identity of the vehicle Vi, where RIDi∈G
- Given the bilinear limitations (P, q,G1,G2, e), the TA selects four unplanned numbers, i.e.,s1, s2, s3, sr∈Z^*q.
- The TA adds PK1 = s1P, PK2 = s2P, and SK^2r = s3P.SKr = Key of RSU.
- The tamper-proof device of each vehicle is in secret preloaded with the parameters {s1, s2, s3}.
- The RSUs are secretly preloaded with the parameters {SK2r ,sr}.

b)Pseudonym and key generation:

1) The RSU computes SKr = srRrand PKr= srP. Therefore, the private key of the RSU can be modeled as (SK1r, SK2r).
2) A vehicle, which is denoted by Vi, chooses a random number ri∈Z∗q.
3) Vi computes ID1i = riPand ID2i = RIDi⊕H(riPK1).
4) Vi computes SK1i = s1ID1i and SK2i =s2H(ID1iID2i).

c)Publishing the system parameters:

The system parameters (*P*, *q*,G1,G2, *e*, *PK*1, *PK*2,*PKr*) are preloaded by each VANET member. The system initialization phase should keep private material confidentiality. First, the private master keys *{s*1, *s*2, *s*3*}* are loaded into the vehicle's tamper-proof device in the system parameter generation process. The tamper-proof device on vehicles, an adversary cannot extract any data stored in the device including key material, data, and code [12]. Second, the tamper-proof device is responsible for generating the identity (*ID*1*i* , *ID*2*i*) and the corresponding privacy key (*SK*1*i* , *SK*2*i*) in the pseudonym and key generation process.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

IV. RESULTS

- **Network Module**

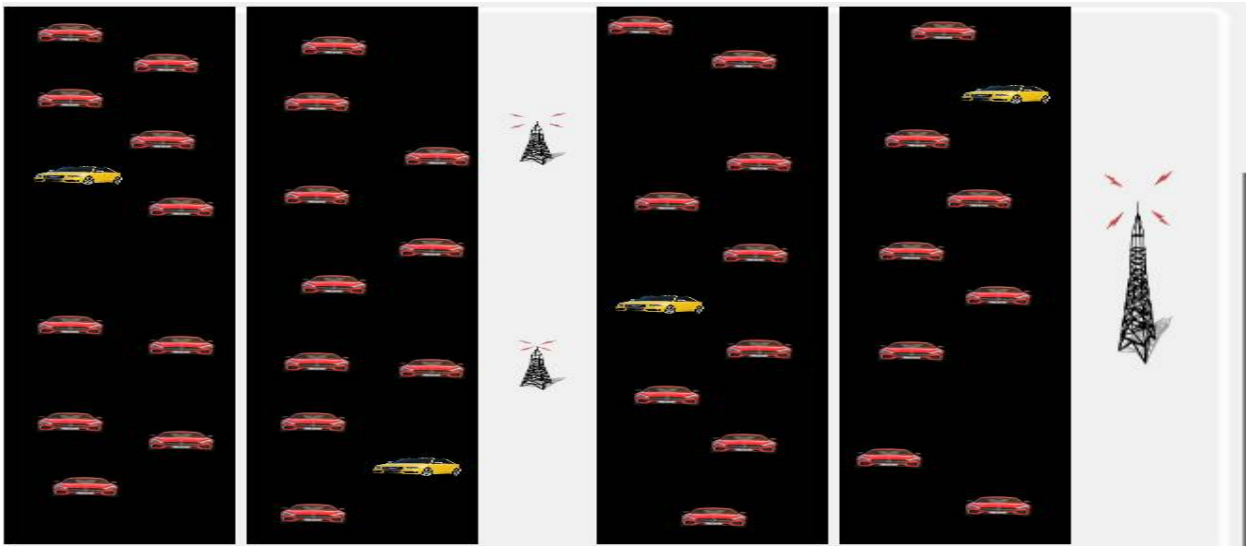


Fig.1 Network

- **Dynamic Key Distribution**

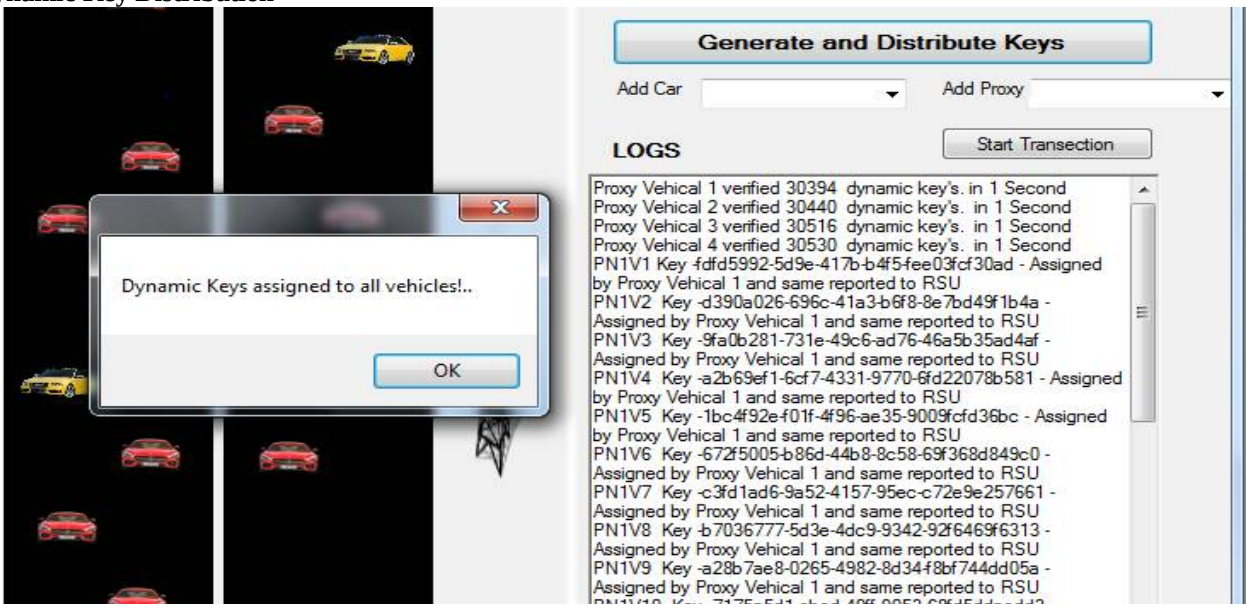


Fig.2 Dynamic key Distribution

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

- **Avoid Redundant Authentication**

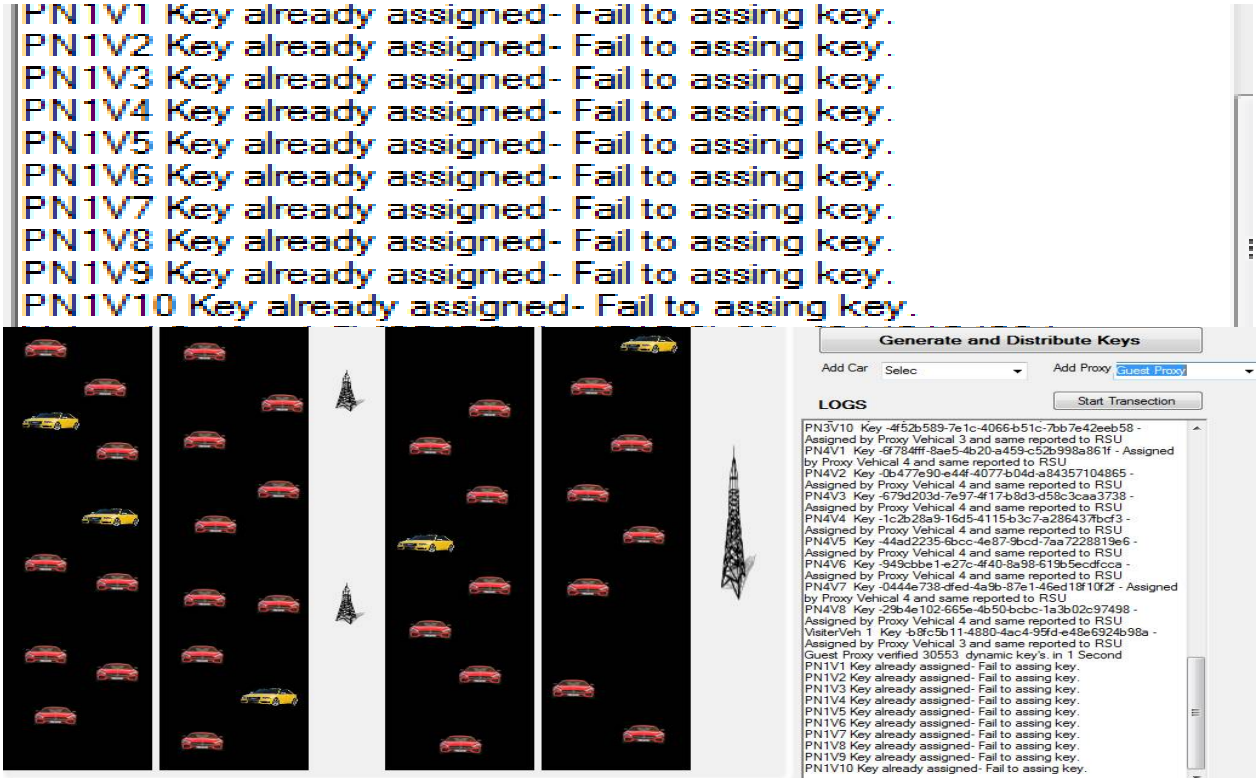
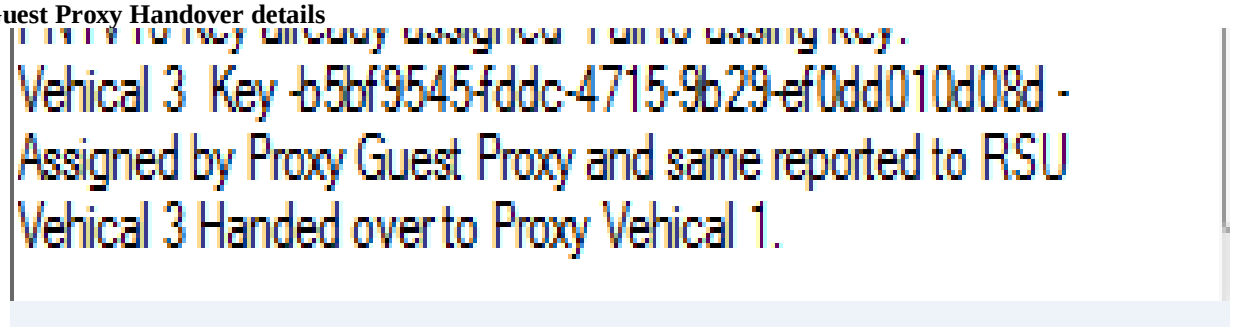


Fig.3 Avoid redundant Authentication

- **Guest Proxy Handover details**



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

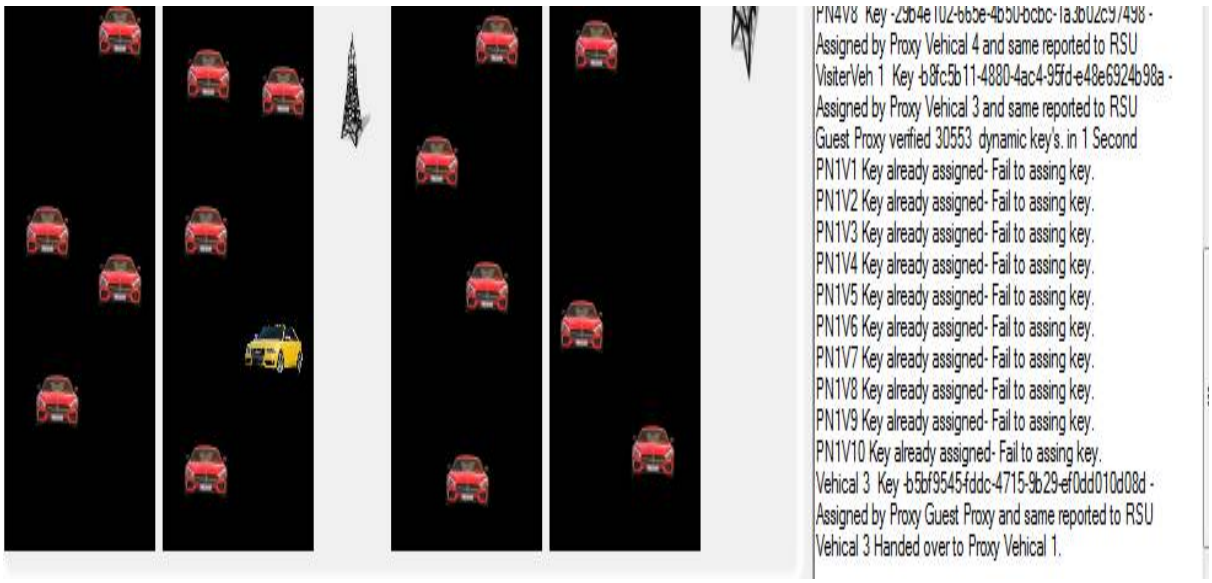


Fig.4 Guest Proxy

V. CONCLUSION

VANET communication is one of most important communication media which is also important for our modern life. The working of Frequent Pattern Tree Algorithm is successfully completed with the help of the properties, those properties are first one is node link property and the another one is attach path property are useful in the data transmission. We successfully completed the proposed system over VANET with following results:

1) Avoid Redundant Authentication of Message.
2) Guest Proxy vehicles are easily handover Record to Regular Proxy.
3) Reuse of Dynamic key are avoided

REFERENCES

[1] A.Nandini,P.VenkateshwaraRao ”Broadcasting message Authentication protocol for Vehicular Ad Hoc Networks using Cluster Technique”IJAEGT ,Volume 2,Issue 09,September ,2014.
[2] FeiWang,Student Member “2FLIP: A Two –Factor Lightweight PrivacyPreserving Authentication Scheme For Vanet”IEEE,yongiunXu,HanwenZhang,Leihuang Zhu ,2015.
[3] A.M.Suhavaneswari ,A.Muthukrishnan “ A Cluster Based Expedite message Authentication Protocol For Vanets”(IJARSE) International Journal of Advanced research In Science and Engineering ,Vol-3,Issue No.4,April 2014,ISSN-2319-8354(E).
[4] YiliangLiu,LiangminWang,Hsiao-HwaChen,Fellow “Message authentication using proxy vehicles in Vehicular ad-hoc Network”,Member,IEEE,Vol-64,No-8,August 2015.
[5] PratabidyaMahapatra,A.Naveena ” A Survey on Identity Based Batch Verification Scheme For Privacy and security in Vanet” ,Vol 3,Issue No.04,April 2016.
[6] Y.Bevishjinila,k.Komathy”An Efficient Authentication Scheme For Vanet Using ChaCheon’s ID Based Signatures” Computer Science ,Volume 4,Issue No.6,June 2014,ISSN-2249-555X.
[7] ShahnawajKhan,NaveenChauhan”Region Authority Collaborated Certificate Organization And Management In VANET”The Third International Conference on Avances in Vehicular Systems,Technology And Applications,Vehicular 2014.
[8] R.Rajan,S.Narendran,M.Prasanth,R.Rajkumar”hybrid Message authentication Protocol In VANET” Computer Science And Information Technologies, Vol. 5,Issue 2,2014,1696-1697,ISSN:0975-9646.
[9] ChenxiZhang,Pin-Han Ho “An Efficient Message Authentication Scheme For vehicular Communications” IEEE,Transaction on Vehicular Technology,Vol.57,No. 6,November 2008.
[10]VinhhoaLA,AnaCAVALLI”Security Attacks And Solutions In vehicular Ad Hoc Networks: a Survey” international journal On Ad Hoc Networking Systems(IJANS) Vol. 4,No 2,April 2014.
[11]Jiun-long huang,Lo-Yao ,hung-Yu Chien “ABAKA:An Anonymous Batch Authenticated And Key Agreement Scheme For Value Added Service In vehicular ad Hoc Networks” IEEE Transctions On Vehicular Technology,Vol. 60,N0.1,January 2011.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

[12]Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin (Sherman) Shen "An Efficient Identity Based Batch Verification Scheme For Vehicular sensor Networks" IEEE Communication Society Subject Matter Expert For Publication In The IEEE Infocom 2008 Proceedings.

[13] Yu-Hsiu Hung, Kai-Hsun ,Wen-Shyong Hsieh "Message Authentication Scheme For Vehicular Ad- Hoc Networks Without RSU" Journal of Information And Multimedia Signal Processing,Volume 6, Number 1,January 2015.

[14] T.S VamsiKrishna,R.Hariharan"VANET-Based Vehicle tacking on Message Authentication And Secure Navigation Route" International Journal Of Computer Application(0975-8887) Volume 113,No. 7,March 2015.

[15] Yong Hao,yuCheng,ChiZhou,Wei Song" A Distributed Key Management Framework With Cooperative Message Authentication In Vanets"IEEE Journal On Specified Areas In communications,Vol.20,No.3,march 2011.

[16] Rinsu Arvind ,Deepa P.L."Secure Authentication For Vehicular Ad –Hoc Network" International Journal Of Computer Science And Technology(IJCST),volume 4,Isue 4,Jul-Aug 2016.

[17] Mohmmad Wazid,Neeraj Kumar,Ashok Kumar Das,vanga odelu,Alavalapti Goutham Reddy,Kisung Park, YoungHo Park,"Design Of LightWeight Authentication And Key Agreement Protocol For Vehicular Ad Hoc Networks" Citation Information :DOI 10.1109/ACCESS.2017.2723265,IEEE Access.

[18] Rukeaiya Y.Shaikh ,Disha Deotale,"Survey On VSPN : VANET –Based And Privacy –preserving Navigation" International Journal of Engineering Research And Applications,ISSN: 2248-9622,Volume 4,Issue 10,October 2014.

[19] Shi-jinn Horng,Shiang-Feng Tzeng,Yi Pan ,Pingzhi Fan,Xian Wang,Tianrui Li,Muhammad khurram khan"b-SPECS+: Batch verification for Secure Psuedonymous authentication In VANET" IEEEtransaction On information forensics And Security,Volume 8,No.11,november 2013.

[20] Khalid abdel hafeez,Lian Zhao,Bobby Ma,JonW. Mark"Performance Analysis And Enhancement Of The DSRC For VANET's Safety Application" IEEE transaction On Vehicular technology ,Volume 62,No. 7,september 2013.

[21] Nitish kumar bharti,Manoj Sindhwani"enhancing The Massage Authentication Process In VANET Under High Traffic condition Using The PBAS Approach" indian Journal Of Science and Technology ,Vol.9(47), ISSN(Print) :0974-6846,DOI:10.17485/ijst/2016/v9i47/106794,December 2016.

[22] Godavari H.kudlikar,Sunita S.Barve"proxy based Batch authentication Scheme For Vehicular Ad-Hoc Network" International Journal Of Computer Science trends and Technology (IJCST)-Volume 4,Issue 3,May-June 2016.