IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-5 E-ISSN: 2347-2693

PBAS: Batch Authentication Scheme for Vehicular Ad Hoc Network using Proxy Vehicle

Godavari H. kudlikar[1*], Sunita S. Barve[2]

[1,2] *Computer Department, Savitribai Phule Pune University, India*

Available online at: www.ijcseonline.org

Received: Apr/21/2016 Revised: May/04/2016 Accepted: May/18/2016 Published: May/31/2016

***Abstract*—**In vehicular ad-hoc networks for authentication Public Key Infrastructure (PKI) was used as Vehicular Signature application. Using PKI scheme integrity of message and identity of senders can be verified. In this scheme task of Road Side Unit (RSU) is to verify received messages one by one, and if this is the case then it is difficult to guess the identity of a vehicle by RSU i.e. from which vehicle particular message is being sent. So Proxy Based Batch Authentication Scheme is being proposed in order to reduce computational overhead of RSU in distributed computing system. In PBAS, each proxy vehicle authenticates multiple messages simultaneously using verification function at the same time, so that RSU can independently verify the outputs given by each proxy vehicles within its range.

***Keywords*—**Proxy vehicle; Proxy based authentication; Privacy preservation; Vehicular ad-hoc network.

I. INTRODUCTION

In this 21st century with huge population each person wants to reach to his working place in right time without considering his safety, So VANET has become a popular topic due to its potential to offer road safety and better driving experience. It also provides certain value-added services such as online facilities, Wi-Fi, vehicles position, direction, speed etc. As communication in VANET is wireless there are certain security issues so certain attacks are possible. Such security attack leads to bad user experience and create drastic consequences. Therefore making VANET secure has become a key objective for designers.

Some of the security schemes like Public key infrastructure (PKI), batch signature verification scheme, Anonymous Batch Authenticated and Key Agreement (ABAKA) scheme, Secure and Privacy Enhancing Communications Scheme(SPECS) have been proposed to make VANET work more efficient. It has also got certain limitations to which are listed below in literature survey along with schemes.

The main goal of this paper is to overcome the above efficiency problem. So this paper is used to design and implement a Proxy Based Batch Authentication Scheme (PBAS) is designed which improves this scheme to some extent by minimizing duplicate message verification i.e. redundant message authentication are minimized. In this scheme, proxy vehicle plays a vital role, were multiple messages can be authenticated using verification function in batch. In addition to this concept of batch key negotiations can be added where RSU verifies output provided by proxy vehicle and then broadcast a single message to all vehicles in RSU range. Following are some of the design requirements of the proposed system:

- The system should ensure message integrity requirement and should be mutually authenticated.
- It should guarantee the freshness of message such that it is resistance to a replay attack.
- The system should meet the requirement of privacy preservation.
- The scheme should be fault tolerant i.e. it should work even for a small number of proxy vehicles.

The remainder of the paper explains as follows: Section II outlines survey related work. Section III describes proposed system architecture, section IV gives details of proposed system in the form of module descriptions. In section V is based system performance analysis followed by results and conclusion made in next two sections.

II. RELATED WORK

Public-Key Infrastructure scheme (PKI) presented by Raya et al. in which RSU verifies messages received by vehicles one by one at any time so it is difficult for road side unit to trace the real identity of a vehicle. Also, this scheme is time-consuming processes and is unable to satisfy the efficiency requirement under continuous changing traffic patterns, which leads to overhead caused due to transmission of a message and computational complexity of on board units if for authentication number of vehicles are increased. In order to improve the efficiency of network Zhang et al. introduced an efficient batch signature verification scheme for communications of vehicles with an external environments like RSUs and this type of communication is vehicle-to-infrastructure. In this scheme instead of verifying messages one by one RSU can verify multiple signatures. Using this scheme RSU can verify near about 1600 messages per sec at a time, so that time required

for verification is reduced to some extent. According to the Dedicated Short Range Communications (DSRC) protocol introduced in [23], it is said that each vehicle broadcasts a traffic safety related message after every 100-300 ms If this is the case than RSU has to verify near about 2500-5000 messages if a number of vehicles considered are around 500. If this is the scenario than batch verification does not satisfy the design requirements.

According to IEEE 1609.2 standard messages sent by each vehicle should be authenticated using the algorithm named Elliptic Curve Digital Signature Algorithm (ECDSA). In this algorithm, it was included that for each message one certificate is required. One of the most challenging things about this algorithm was to find a way such that while computation and transmission less amount of resource should be consumed. Another limitation of this algorithm is it does not overcome security attacks and for calculation most expensive operations are used such as modular inversion, scalar multiplication and there are chances of message delay and message loss rate.

A Secure and Privacy Enhancing Communications Scheme (SPECS), introduced by Chim *et al.* here in this scheme after batch authentication, a group of vehicles is formed and they communicate with one other confidentially and it differentiates scheme with other as while communication between vehicles RSUs are not included and this protocol is called as group communication protocol. Limitation of using this scheme is that it is most prone to impersonation attacks. In this scheme, it is possible that any malicious vehicle or fake vehicle can act as trusted entity and has the ability to broadcast any fake messages to all other vehicles. It not only sends false messages but also force other vehicles which are belonging to another group to send messages securely to each other. These limitations are observed by Horng and to this, some additional work done on this scheme b-SPECS+ scheme was proposed. In this scheme certain assumptions were made such as Trusted Authority should work always online and no single point failure is observed.

Li et al. proposed a scheme named Rapid Certification Scheme (RCS) and Shim et al. also proposed a scheme Conditional Privacy Preserving Authentication Scheme (CPAS). In RCS, one leader is assigned for a specific range and named as VANET leader. Task of this VANET leader is to collect all the sent messages from each vehicle and send those all messages to Road Side Unit. In CPAS for each message a pseudo identity is assigned and Task of TA is to regain real identity. As batch signature, verification is done within less time so the time required for verification is reduced to some extent. Instead of using MapToPoint function this scheme uses hash function so efficiency is not good. Using batch verification process it can verify near about 750 signatures in about 300 ms.

Earlier for each message certificate was being assigned If we consider 500 vehicles sending safety related messages after every 300ms those many certificates need to be assigned. If this is the case large amount of space is required for storage purpose so Albert et al. their work introduced a protocol called expedite message authentication protocol(EMAP). Use of this protocol is that whenever any new vehicle comes into system range certificate of that vehicle need to be checked, and this should be done for each vehicle. So to cope up with this problem Expedite Message Authentication Protocol is being introduced. This protocol acts as an alternative to Certification Revocation List checking process and this can be done by using secure Hash MAC function i.e. Hash Message Authentication Code function. This protocol not only suites for Vehicular Ad Hoc Network but also it is suitable for any network consisting to Public Key Infrastructure for reducing authentication delay which is caused by certificate revocation list checking. Another advantage of using this protocol is that it uses novel key distribution probability were a secret secure key is distributed or shared by On Board Unit which are non-revoked which is also updated timely. Message loss ratio i.e. number of messages dropped while the transmission is reduced if this protocol is used. Certain research and analysis are being made on this protocol working and based on this analysis it is concluded that this protocol is secure and efficient protocol.

Another protocol named medium Access Control protocol is being introduced were using this protocol passengers present inside the vehicle can surf the internet and also various additional services can be provided. This protocol uses time stamp mechanism were updated data is provided so that it guarantee the freshness of message.

III. PROPOSED ARCHITECTURE

Proxy Based Batch Authentication Scheme consists of components named Vehicles, Trusted Authority, Proxy Vehicles and Road Side Unit. In this system main role is played by proxy vehicles as it performs batch signature verification. As shown in the fig.1 architecture of system consist of the components were for each component-specific task is assigned. Firstly system initialization takes place and all the parameters are initialised and this all is done by Trust Authority. All the private keys, pseudo identity keys are initialised for each vehicle connected in the system. Likewise, Vehicles send their messages for message signing contains information related to their present location, speed, directions etc. All these messages are first signed using signatures generated by vehicles and tamper proof devices. After signing of messages they are sent to a nearby proxy vehicle for batch verification were multiple messages are authenticated using some verification function. Using this technique centralized computing load is distributed to a

number of the proxy vehicle which ultimately decreases the computational load on RSU. After successful batch authentication, results are sent to RSU were the validity of results are checked.

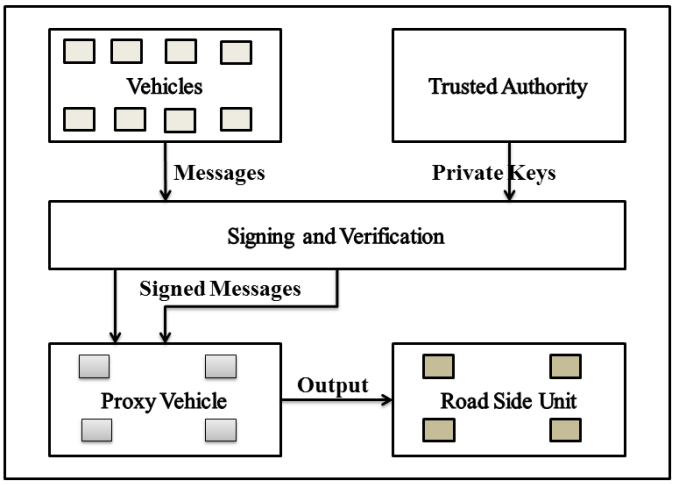

Fig. 1 Architecture for PBAS

In this proposed scheme if the following task is done properly then all the design requirements like message integrity, authentication, privacy preservation and computational efficiency requirements are full field.

IV. System Module

The proposed system consists of four modules those can also be called as phases of the algorithm. Description for each module is as listed below.

A. *Initialization phase*

This step is an essential step in which system is initialized with the parameters which are used for the purpose of authentication. Calculation regarding all the required keys like public and private keys are done separately and stored. It can be mathematically modeled as follows:

- Tamper proof device preloads each vehicle with three master keys {mas1, mas2, mas3}.
- Trusted Authority computes public and private keys {P1, P2} and {S1, S2} along with pseudo id keys {PID1, PID2}.
- All these parameters are preloaded by each member of system.

B. *Message Signing Phase*

The main objective of this phase is to ensure message integrity and to also check the validity of each vehicle. This can be done by signing the message with the private secure key such that it is known only by TA. It is different from another scheme because here for the signing of message both public and private keys are used. Tamper proof device generates a signature. Both this generated signatures are used for batch verification.

C. *Batch Verification phase using proxy vehicles*

In this phase, the first task is to select an appropriate proxy vehicle, the vehicle having low computing capability can be selected a proxy vehicle. After a number of proxy vehicles are set vehicles nearer to proxy vehicles sends their signed message for authentication purpose. This proxy vehicle collects messages from a vehicle and after receiving sent messages batch authentication is done. Selection strategy for proxy vehicle can be of many types which are as listed below

- The vehicle having extra resources as compared to other, that vehicle can be selected as proxy vehicle.
- Certain fixed number of a proxy vehicle is assigned.

The role of a proxy vehicle is to verify those sent messages and it can be done using bilinear mapping. Also, there are no limitations to number of proxy vehicles.

D. *Output Verification Phase at Road Side Units*

In this phase, RSU verifies the sent results from proxy vehicles independently. Here in this module it mainly checks for false results and also to check whether proxy vehicles are real proxy vehicles. It includes three tasks first one is check for a real proxy vehicle, the second task is to check for proper result wether data is altered or modified, the third task includes revoking of a proxy vehicle if malicious proxy vehicle found.

After batch verification done successfully results are sent to RSU, it includes Pseudo identity key for the proxy vehicle along with a signature of the proxy vehicle and verified message. To check for the proper working of task following steps are performed.

- Road Side Unit checks for the signature of a proxy vehicle if it is valid then it is concluded that vehicle is a real proxy vehicle.
- The signature generated by tamper proof is signed with a key of RSU and is compared with hashed message, signature and pseudo identity. If both this terms matches it means that results are valid.
- If above condition not satisfied it means that vehicle is false vehicle so it revokes proxy vehicle.

V. Security Performance

In this section analysis regarding PBAS is done using following aspects like the integrity of the message, authentication, guarantee freshness of message, privacy preservation etc.

A. Integrity of message and authentication:
The system is authenticated as vehicle and tamper proof device independently generates a signature using privacy keys. So even if an external attacker tries to access the data it is difficult without knowing privacy keys.
Also, while batch authentication signatures of each vehicle are checked with signature generated by tamper proof device if both this signatures are valid it means integrity of message is maintained.

B. Guarantee freshness of message:
Based on arrival time and departure time of received message it is decided whether to drop the message or to forward the message to a proxy vehicle.

C. *Fault Tolerance:*
This scheme has the ability to verify messages and continue verification process even if a number of proxy vehicles is small.

VI. EXPERIMENTAL RESULTS

Below are results which were evaluated after executing system several time based on those results analysis were made.

A. Computational Overhead Analysis
Below graph in Fig.2 clarifies the relationship between number of messages and amount of time required for verifying signature. It evaluates the performance of system by comparing PBAS with contribution i.e. additional efforts made in this previous scheme in order to improve efficiency in terms of computational overheads for road side unit. From fig it can be determine that with increase in number of messages computational overhead increases.
Contribution is additional efforts on PBAS which consist of reducing redundant authentication. As compared to contribution in PBAS number of messages to be verified is large as compared to our system. So in contribution computational overheads are less. It mainly depends on three factors T_{hash} time needed to perform MapToPoint Hash operation, T_{mult} time to perform pairing and T_{pair} time to perform one point multiplication. There values are calculated and are set constant 0.39, 0.09 and 3.21 respectively. It can be mathematically represented as follows, as after 300ms traffic related messages are broadcasted so a value of m is calculated using below equation.

$$2mT_{mult}+(2m+3)T_{pair}+T_{Hash}$$

Where, m = [number of messages\ 300]

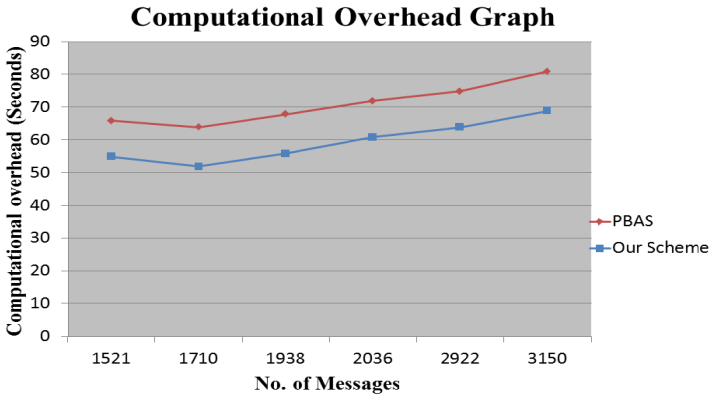

Fig.2 Performance comparison of schemes in terms of computational overhead

B. Transmission Overhead Analysis
Next graph analyzes transmission overhead; here in Fig. 3 relationship between a number of messages and transmission overheads in bytes is shown. It mainly focuses on the size of the message in terms of bytes as compared to previous work mentioned. The packet size of a message sent by proxy vehicles to road side unit is 126bytes and that of message sent from RSU is 42 bytes. Total bytes required to send a message from proxy vehicle to RSU is 126+42 and for sending n messages 126+42n bytes are required. So based on this calculations Transmission overhead is determined.

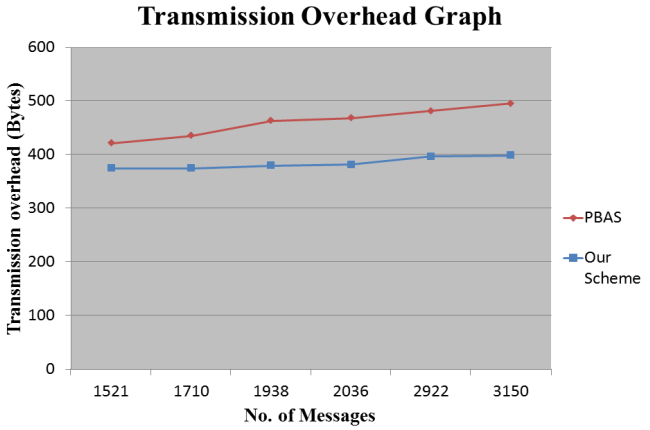

Fig.3 Performance comparison of schemes in terms of transmission overhead

As per the efforts made in PBAS number of messages to be verified is less in the contribution even if a proxy vehicle and a total number of vehicles are same.

C. Average Message Delay Analysis
Fig.4 shows the set of simulation results in terms of message delay. It gives details about average message delay analysis which shows a relationship between a number of vehicles and time required to transmit messages from vehicle to RSU. As per the analysis made in previous schemes like IBV, CPAS, ABAKA performance of PBAS

is good as this scheme reduces the number of handshakes between vehicles and RSU. Here each vehicle is distributed over different lanes and speed should be between 30-60 m/s.

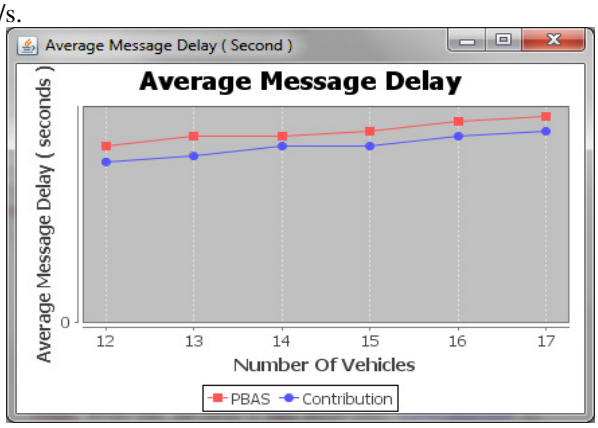

Fig. 4 comparison of schemes in terms of message delay ratio

VII. CONCLUSION

As per the research made on this scheme and after evaluating results it is observed that by making additional efforts like reducing redundant authentication on PBAS performance and efficiency of a system is increased by 20-25%. And based on the above results and performance evaluations it can be concluded that computational overheads as well as transmission overheads on RSU are reduced.

ACKNOWLEDGMENT *(HEADING 5)*

I would like to thanks, Prof. Sunita S. Barve for giving her valuable guidance. Thanks to all the computer department professors and staff who continuously and indirectly supported, inspired me to keep working on this system.

REFERENCES

[1] Chim T.W, Yiu, S.M, Hui Li, "VSPN: VANET-Based Secure and Privacy Preserving Navigation", IEEE Transactions on Computers, vol.63, no.2, (2014):pp.510-524

[2] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, vol.63, no.2,(2014): pp.907-919

[3] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero "VANET security surveys", in Computer Communications, vol.44, no.4,(2014): pp 1–13

[4] Lamba S; Sharma M., "An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)", International Conference on Machine Intelligence and Research Advancement (ICMIRA), (2013): pp.179-183

[5] Wasef, A.; Xuemin Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol.12, no.1,(2013): pp.78-89

[6] Xiaodong Lin; Xu Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, vol.62, no.7, (2013):pp.3339-3348

[7] Shi-Jinn Horng; Shiang-Feng Tzeng; Yi Pan; Pingzhi Fan; Xian Wang; Tianrui Li; Khan, M.K., " b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET ", IEEE Transactions on Information Forensics and Security, vol.8, no.11,(2013): pp.1860-1875

[8] IEEE Standard for "Wireless Access in Vehicular Environments Security Services for Applications and Management Messages", on IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006) , (2013):pp.1-289

[9] Rongxing Lu; Xiaodong Lin; Zhiguo Shi; Shen, X.S., "A Lightweight Conditional Privacy-Preservation Protocol for Vehicular Traffic-Monitoring Systems" IEEE in Intelligent Systems , vol.28, no.3(2013): pp.62-65

[10] Dietzel, S.; Petit, J.; Heijenk, G.; Kargl, F., " Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols", IEEE Transactions on Vehicular Technology, vol.62, no.4,(2013): pp.1505-1518

[11] Xiaojun Li; Liangmin Wang, "A Rapid Certification Protocol from Bilinear Pairings for Vehicular Ad Hoc Networks" in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , (2012):pp.890-895

[12] Rongxing Lu; Xiaodong Li; Luan, T.H.; Xiaohui Liang; Xuemin Shen, " Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs" , IEEE Transactions on Vehicular Technology , vol.61, no.1,(2012): pp.86-96

[13] Kyung-Ah Shim, " CPAS : An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks", IEEE Transactions on Vehicular Technology, vol.61, no.4, (2012):pp.1874-1883

[14] Jiun-Long Huang; Lo-Yao Yeh; Hung-Yu Chien, " ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks", in Vehicular Technology, IEEE Transactions on , vol.60, no.1, pp.248-262, Jan. 2011

[15] Lingbo Wei; Jianwei Liu; Tingge Zhu, " On a Group Signature Scheme Supporting Batch Verification for Vehicular Networks", in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on ,(2011):pp.436-440

[16] T. W. Chim, S. M. Yiu, C. K. Hui, and O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs", Ad Hoc Networks, vol.9, Issue.2,(2011): pp.189-203

[17] Isaac, J.T.; Zeadally, S.; Camara, J.S., "Security attacks and solutions for vehicular ad hoc networks", IEEE Transaction in Communications, vol.4, no.7,(2010):pp.894-903

[18] Yipin Sun; Rongxing Lu; Xiaodong Lin; Xuemin Shen; Jinshu Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications", IEEE Transactions on Vehicular Technology, vol.59, no.7, (2010):pp.3589-3603

[19] Ghassan Samara, Wafaa A. H. Al-Salihy, R. Sures., "Security analysis of vehicular ad hoc networks (VANET)", in IEEE Conf. Network Applications Protocols and Services (NETAPPS), (2010):pp.55-60

[20] Wasef, A.; Rongxing Lu; Xiaodong Lin; Xuemin Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]" , IEEE Transaction on Wireless Communications, vol.17, no.5,(2010): pp.22-28

[21] Wasef, A.; Yixin Jiang; Xuemin Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks" IEEE Transactions on Vehicular Technology, vol.59, no.2,(2010): pp.533-549

[22] C. Zhang; R. Lu; X. Lin; P. Ho; X. Shen., "An efficient identity-based batch verification scheme for vehicular sensor networks", IEEE INFOCOM in Proc.,(2008):pp. 246-250