VOL. 10, NO 20, NOVEMBER, 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

EFFICIENT PRIVACY PRESERVING AUTHENTICATION FOR VEHICULAR AD-HOC NETWORKS

S. Supriya[1] and B. Bharathi[2]
[1]Murugappa Polytechnic College, Chennai, India
[2]Faculty of Computing, Sathyabama University, Chennai, India
E-Mail: dssupriyaa@yahoo.co.in

ABSTRACT

Vehicular networks are a fast developing research topic which is useful for the area like traffic efficiency enhancement and safety application. VANET (Vehicular Ad-Hoc Network) is considered as an intelligent transport system where in the vehicles can able to communicate with each other and also with the road side infrastructure. Since the message exchange between two vehicles are ad-hoc in nature and the driver behavior and high mobility of the vehicle, there is a chance of privacy and security problems and also the authentication is an another issue for any secured interactions due to the VANET has a unsecured and untrusted nature. The paper reviews various existing authentication protocols used for efficient privacy preserving authentication in the VANET.

Keywords: VANET (Vehicular Ad-Hoc Network), authentication, privacy preserving.

1. INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is another form of Mobile Ad Hoc Network in which the nodes can change their location independently within the coverage area and they can communicate with other nodes without any fixed infrastructure. The nodes in the VANET may include a vehicle, or Road Side Unit (RSU). Hence the VANET technology provides good traffic efficiency and road safety. The vehicles are equipped with the on-board Unit (OBU) device which performs the communication in the VANET where in the huge self-organized network communication is performed.

Normally the VANET bring the drivers of the vehicle a pervasive environment that provides many services. VANET provides safety driving and comfort to the drivers in the network. A vehicle in the network transfer its traffic information to all others vehicle in the network that makes other vehicles to avoid accidents in advance. In addition, the vehicles can able to share some other information like tourism information, hotel information, movie files which make their journey more comfortable. Because of the enormous application of VANET, it becomes a research topic in many industries. Even though the VANET have many advantages and useful applications to implement, it has some authentication, security and privacy preserving issues that must be addressed and resolved.

There are many security requirements to be satisfied by the VANET environment which include sender authentication to provide that the message is received from the valid person, privacy preserving which maintain the message between sender and receiver in private and also protect the route of the vehicle which should not be traced by other unauthorized party. If the security and privacy preserving setting are not delineated genuinely, then the real identity of the vehicle is found which leads to fraudulent activity.

2. SECURITY REQUIREMENTS IN VANET

The security design of VANET should assure the following:

a) Authentication

The message transfer among the vehicles should be authenticated periodically using the authentication certificate. This authentication ensure about the origin and their authentication level. The vehicle in the VANET gives a private key with every message along with the certificate. On the other end, the receiver receives the message and authenticates the certificate and the key and finally evaluates the message. This leads to the overhead that every time the message authentication with different key is performed. Mostly this type of overhead is reduced by using the efficient public key cryptographic techniques.

b) Availability

The VANET network must be available all the time. Suppose the application incorporates emergency information to be transferring to another vehicle which has more probability to meet accident, this needs a quick response from the network to pass the information. A delay less than a second may cause severe damage and result in meaningless message. This may lead to network vulnerable to Denial of Service (DoS) attack. This can be overcome by store the partial message in the intermediate hops and that will be completed during upcoming transmission.

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

c) Non-repudiation

Non-repudiation makes the vehicle to find the attackers in the network who send the false messages. This supports the network during cheater do their crime activity. Considering the VANET, the emergency alert messages have been stored in the tamper proof device (TPD) and the officially authorized vehicle can only able to retrieve the data.

d) Privacy

Prevent the information from the unauthorized people is called as privacy. This information may include route of the vehicle, speed per hour, driver identity, etc. usually the privacy is done by using the temporary key which can be changed periodically. These key are stored in the TPD for the future use. To prevent the identity of the vehicle, the Electronic License Plate (ELP) is used to provide the identification number of the particular vehicle.

e) Confidentiality

All the drivers should maintain the privacy. The messages between the vehicles contain the driver information that should be encrypted and prevented from the attackers.

There are many existing Privacy Preserving Authentication (PPA) schemes and methods used for the Vehicular Ad-Hoc Network are available. The following session reviews those PPA in VANET.

3. METHODS AND SCHEMES USED FOR EFFICIENT PRIVACY PRESERVING AUTHENTICATION (PPA)

a) Efficient privacy preserving authentication protocol

The Efficient Privacy Preserving Authentication Protocol (Hu Xiong, *et al*., 2010) proposes two counter measures that act against the fraudulent messages created by the malicious vehicles. They are posteriori and priori. In the posteriori remedy, the Trusted Authority (TA) is having the ability to find the real identity of OBU targeted to discuss the traffic events. This is possible for the trusted authority alone, but the public cannot find the real identity of any node on implementing posteriori remedy. The second one is priori which is capable of preventing the fraudulent message generation. In this method, the receiver will accept the received message as valid only if the message has been supported by some vehicle more than the threshold. The Efficient Privacy Preserving Authentication Protocol has achieved the posteriori and priori remedies, efficiency and threshold-adaptivity.

The Efficient Privacy Preserving Authentication Protocol scheme has the four sequential steps namely: system initialization, OBU Safety Message Generation, Message Verification and OBU fast tracing. The Trusted Authority (TA) design the signature from the On-Board Unit (OBU) and the Road Side Unit (RSU) translate that signature. The signature is again delegated with respect to the TA public key and stores the re-signature in the RSU. On the receiver side, the receiver receives the message and resigns it using re-signature key after validation. There is possibility that any malicious vehicle in the networks can able to verify the message and use the information. So the proxy re-signature is used to cover the identity of the real OBU. This protocol is the extension of proxy re-signature scheme which also maintains the conditional anonymity authentication with trust worthy.

b) ECPP: Efficient conditional privacy preservation protocol

The Efficient Conditional Privacy Preservation Protocol (Rongxing Lu, *et al*., 2008) is used to overcome the anonymous authentication of safety massages along with authority tracing. This system provides short time anonymous key between OBU and RSU to fast anonymous authentication and privacy tracking. The ECPP protocol has four steps to achieve fast authentication and conditional privacy. They are system initialization; OBU short time anonymous key generation, OBU safety message generation, OBU fast tracking algorithm.

The Trusted Authority TA attains the identity of RBU and OBU and provides the private key to the requester. Consider on the first portion that the requester is RSU, and then the private key has the location awareness key followed by the anonymous signing key. Suppose that the requester is OBU, then the private key contains the pseudo id generated from the real identity of the requester and an identity based private key from the pseudo id. In the second step, the OBU send a request for generating the short time anonymous key whenever the OBU is passing through the RBU. The OBU got the request of RBU and check the particular OBU is in revocation list of RBU. This provides the network from revocation issue of OBU which takes large storage space for that revocation list. Once the short time anonymous key is gained, then the third step is to send the safety message within the short time mentioned in the previous steps.

On the fourth step of the protocol, a fast tracking algorithm is implemented for tracking the OBU of the attained safety message. With the support of the safety message, the TA use the master key to get the position of RSU which issued the safety message and the process is reversed to get the original location of the RBU and OBU. The ECPP protocol is used for the secure vehicular communication with the short time anonymous key generation and provides the conditional privacy preserving, improves efficiency fast verification of safety message and an efficient privacy tracking mechanism.

c) An improved mutual authenticated privacy-preserving protocol

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

The VANET is termed as mutual authenticated privacy preserving network only if the communication in the network satisfies the security properties such as Mutual authentication, anonymity, un-linkability and traceability. The new privacy preserving mutual authentication protocol (Zuowen Tan, 2010) has six main steps to satisfy the mentioned security properties. First step is initialization where in the master key and the generator is chosen and the public key is computed and published, this public key issue the group key to all the RSU. The Trust Center (TC) also updates the group key. The second step is registration, all the vehicle in the network register in Vehicle Administrative Center. Then the TC encode the identity of the vehicle with its public key and it computes the private key for each vehicle, sends to the respective vehicle along the secure channel.

Next the OBU request the nearest RSU for the anonymous certificate, then the RSU response the request in the specified way. While receiving the signatures from RSU, the OBU computes many short time anonymous certificates from RSU. Thus the communication between the vehicles is possible by providing the short time anonymous certificates every time without requesting the RSU all the time. The OBU checks the new short time anonymous certificate in terms of validity of the public key, validity of the certificate and then the validity of the message. Finally once all the verification and validation is done, the TC traces the RSU and OBU by using the Malicious Participants' Trace operations. Thus in the proposed protocol has three main mechanism in it. They are secure identity-based group blind signature, public encryption, and a private encryption in final. The malicious nodes (RSU and OBU) can be easily traced by the Trusted Center using this protocol.

d) Distributed Vehicular Public Key Infrastructure (VPKI)

Vehicular Public Key Infrastructure (VPKI) (Mahalakshmi.R.S, and Alangudi Balaji.N, 2014) is used to overcome the location privacy and the vehicle anonymity problem during vehicle communication. Usually the vehicles in the VANET are having the inbuilt temper-resistant crypto-module where in the packet authentication is not possible. The attackers in the network easily gain the legitimate identity and modify or replay the messages. This action leads to the malicious behaviour which is a crucial problem in the security of VANET.

Hence a Vehicular Public Key Infrastructure (VPKI) is implemented in the VANET environment which has the primary function to observe and detect the abnormal nodes or activity in the network. This infrastructure uses a certification authority which holds the user identities along with the respective public key. In addition the VPKI includes the RSA key generation techniques which is useful in terms of authentication and security. The RSA is a public key algorithm comprises of two keys namely public key and private key. The private key is a secret key whereas public key can be shared by any vehicle in the network. The privacy information is encrypted by using the public key and the on the receiving side the encrypted information is decrypted using the private key. Both the keys are having mathematically relationship but the private key computation using public key is not possible. Thus the proposed VPKI scheme along with the RSA algorithm is used to preserve the location information of the vehicles those sharing messages safely and also it prevents the vehicle communication against the vehicle anonymity.

e) Privacy-preserving authentication protocols based on self-certificate signature

VANET is considered as a significant Intelligent Transport system (ITS) where the people in the vehicles can able to have comfortable and safe journey. Initially the groups oriented signature and Pseudonyms techniques are used for the privacy preserving in the VANET. But these two techniques fail with some disadvantages that may crash the communication and even the network. Hence a new privacy preserving authentication protocol (Jianhong Zhang, *et al.*, 2012) with Self-Certified Signature is introduced to overcome those existing problems.

The privacy preserving authentication scheme based on Self-Certificate Signature starts with the system initialization where the Trusted Authority TA selects the master key using the bilinear map of the network and calculates the public key. The two collision resistant hash functions are selected and a secret member list of the network is maintained. In the second step, the vehicle which needs to join the VANET should communicate with the TA along with its original identity via secure channel. The third step is to provide the anonymous authentication. The vehicles communication is achieved through sending messages. These messages have standard necessary fields such as message-ID, payload, Timestamp, TTL and signature. The message-ID indicates the message type, payload is the actual message to convey, timestamp includes the time at when the message produce and support to prevent from replay attacks, TTL is Time to live which show the time being the message can stay in the network, signature is for authentication process which has some valid steps to produce. Fourth step is to verify the signature generated in the previous step. Finally the message which is having forged signature is kept under tracing which find the location of the malicious message generation.

f) Secure and efficient protocol for vehicular ad-hoc network

There are many protocols and methods are available for the privacy preserving and authenticated communication between the vehicles in the VANET. All these existing systems have done their work in reliable and efficient manner. But still they the many drawbacks such

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

as the large storage space requires for the storing the revocation list and the pseudonym needs to be verified and stored each time, the authentication process takes more time to process on both the sender and receiver side. The revoked vehicles list is maintained and update to all the nodes periodically, therefore, the computational complexities and the communicational overhead increased.

Hence, the Secure and Efficient Protocol for Vehicular Ad-Hoc Network (Bharati Mishra, *et al*., 2011) is introduced which provide message authentication and conditional privacy preserving. Initially the vehicles in the VANET register their identity with the Trusted Authority TA by providing the original identity, proof, etc. after verifying the identities provided, the vehicle owner generate their public-private key pairs using the specified algorithm. Then the TA provides the certificates which authenticate the fresh set of public keys. The third party can only validate the certificate using these public keys. The RSU is placed in the road side by the transport authority by which the entire vehicle details are updated to the RSU and the TA registered with the RSA provides its public key for communication. So the RSU is working as an intermediate between the network vehicles and the TA. In addition this protocol scheme provides the message transfer method in two conditions (i.e.) the destination is in the range of RSU and the destination is out of the range of RSU. Hence, by facilitating all these steps the secure and efficient protocol for the message authentication and privacy preserving, the vehicles in the network is employed with the secure driving with assure privacy preserving communication environment.

g) Protocol for quick message authentication in vehicular network

In VANET, a sender sends information the receiver in a secure manner. On the receiving side, the receiver checks the sender certificate which includes the revocation status checking, verifying the sender certificate and finally the sender signature verification. The Certification Revocation List (CRL) size needs to be spacious which lead to the delay during the revocation status checking in the received message. Hence a quick message authentication protocol (M. Ramya and N. Mohanapriya, 2014) is introduced to reduce the delay in authentication. It makes use of the Hasten authentication process to decrease the time delay and make the communication in the VANET more secure.

The proposed system uses the six sequential steps to achieve quick and secure authentication of messages between the vehicles. First step is system initialization where the primary security requirements are verified. Then the message authentication is done using the proposed TACK scheme for authentication and revocation. It includes the central trusted authority for storing the details of each vehicle and the regional authority where vehicle register its certificate. Both the revocation authorities and the trusted authority present all over the network. The third step is all about revocation where the conventional PKI process checks the CRL for the entire received message immediately after receiving. Fourth step is security analysis where in the secret key is leaked and the revocation process is done by computing the received message HMAC values. This method saves the new secret key in the HSM (tamper resistant). This new secret key cannot be able to tamper in any condition. Fifth step is verifying the delay. This is done using the Elliptic Curve Digital Signature Algorithm (ECDSA). Sixth step is to measure the end-to-end delay. And the final step is measuring the message loss ratio. It is the ratio between the numbers of message dropped due to the authentication delay using the proposed protocol. The paper utilizes the Hasten which can reduce the message loss and delays due to authentication when compared to the conventional methods and algorithms.

h) Aggregate privacy preserving authentication in VANET

The privacy preserving and security protocols used in VANET has contain large volume of cryptographic data and operations. This leads to the problem of processing the large volume of data while receiving the message. Hence the proposed Aggregate Privacy Preserving Authentication protocol (Lei Zhang, e*t al*., 2011) is suggested to overcome this problem. This protocol has designed with the global security, individual privacy and the easy implementation as its design goals.

The protocol is based on the one-time identity-based aggregate signature (OTIBAS) scheme which comprises of the identity-based cryptography, aggregate signature and the one-time signature. This scheme aggregates different efficient algorithm process such as Setup, Extract, Sign, Aggregate and Verify. Setup intake the security parameter and provides the global system parameters along with the public key of Trusted Authority TA. In Extract session, the master secret key of TA and the vehicle identity is taken as input, provides the signer's private key. Sign intakes that signer's private key, collects the message from the vehicle and produce the signature on the message. This signer's private key is valid for generating one signature. Aggregate simply collects the number of messages and the signature from the Sign step and generate an aggregate signature. Final Verify step takes the output of all the above steps in OTIBAS scheme, verify it whether the message with the signatures are valid or not. Thus the protocol provides secure and privacy preserving vehicle communication. It reduces the delay in message processing and compresses the cryptographic data which saves the storage space of the vehicle.

i) Authentication scheme for emergency communication in VANET

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

Most of the scheme and protocols used in the VANET is mainly concentrated to satisfy privacy requirements. But the message verification is not taken as serious as practical. Hence the Efficient Privacy-preserving Authentication Scheme (EPAS) (Xuedan Jia, *et al*., 2013) is used to alert or send message in period of emergency. The proposed scheme is very challenging for the real-time environment without fixed Road Side Units (RSU). The protocol overcome the privacy preserving problem by employing the EPAS which is an identity based signature scheme and provide message authentication by light weight signature and batch verification processes.

The EPAS is having the initial two steps such as system initialization and vehicle registration as other protocols possess. Then it uses identity based cryptography where in the public key of the vehicle is generated based on its identity. This procedure has no certificate management and transportation. Therefore, the communication overhead and computational complexity are reduced considerably. Pseudonym is generated to get the message along with the signature which protects the location of the vehicle from being tracked. Then the session key is generated using Diffie-Hellman session key agreement scheme and the mutual authentication is achieved between the network vehicles and the Disaster Relief Authority (DRA) vehicles. The EPAS scheme has two sub-schemes. Scheme: 1 is for the Vehicle to DRA (V2D) communication where the trust percentage of DRA is high and the private key alone is not sufficient to retrieve the real identity of the vehicle and the pseudonym value of a vehicle change time to time. Scheme: 2 is Vehicle Group Communication where the verification process is fast enough to reduce the computational overhead during emergency.

j) Authentication overhead reduction in fast roaming networks

Two important authentication schemes such as roaming Proxy Re-encryption Authentication scheme and a new proxy re-encryption scheme are used to reduce the authentication overhead. The concept of Proxy Re-encryption Authentication scheme is that the cipher texts to be send to service provider is encrypted by its public key and transformed by a proxy as cipher text of a vehicle in the network and that can be decrypted by using the vehicle's private key. This process is normally happen in cryptography. But the authentication scheme implements to provide the re-encryption key used for the proxy to transform the cipher text to the service provider. This scheme is efficient to some extent. But it leads to many attacks in the VANET such as Denial of Service, Masquerade, Tamper-proof device, Eavesdropping and Key bootstrapping and rekeying.

To minimize the attacks in the Proxy Re-encryption method, a new Proxy Re-encryption authentication scheme (Surabhi Mahajan and Alka Jindal, 2010) is proposed. This new scheme is also have the same functionality as the previous scheme has, but the message encryption using the public key is done using the private key here. This private is known only to the car and the access point (AP) and it cannot be replayed by the attacker. Hence the message between the car and the access point is transmitted securely after authentication. This new scheme is also vulnerable to attacks such as Denial of Service and Eavesdropping. Thus the newly proposed scheme provides security, authentication, and privacy and reduces overheads in the fast roaming networks.

k) Privacy schemes in VANET

Among the security requirements in VANET, privacy is the important issue to be resolved. The paper (Sapna S. Kaushik, 2013) reviews different approaches used to prevent the privacy in VANET. Five approaches of the paper are reviewed here. As the location of the vehicle in VANET changes dynamically, the pseudonyms value is also changes rapidly. Therefore, there is a chance of attack that links the old and new pseudonyms. Hence the mix zone techniques (J. Freudiger, *et al*., 2007) are implemented along with the silent period scheme (L.Huang, *et al*., 2005) that improves the pseudonyms schemes against such attacks. Another method is proposed to prevent the location privacy in VANET called Group Signature method where a public key is associated with the multiple private keys of the members in the group. The advantage is that the eavesdropper can able to know only the group public key but the location of message sender is kept secret which cannot be retrieved. (X. Lin, *et al*., 2007) show the method to implement the group signature protocol in the VANET systematically.

The vehicles in the VANET form groups (K.Sampigethava, *et al*., 2007) based on its location and roaming speed. Every group has a group leader who sacrifices its own privacy and forwards the messages of the group members. This method is high expensive in nature and it has the chance of electing the malicious node as a group manager, this leads to the privacy leakage of the group members also. Therefore, this scheme provides poor privacy and leads to the remove the concept of group manager. Instead a signature is created (Brijesh Kumar Chaurasia, *et al*., 2011), for the whole group using the public keys of the group members. This is useful in terms of sending message but it is an unconditional privacy scheme since it does not provide non repudiation.

l) Priority-based verification of VANET safety messages

The paper (Subir Biswas and Jelena Misic, 2013) presents the priority-based safety message verification in VANET which comprises of message authentication and the prioritized verification of road safety messages as the message verification time is longer in VANET. In the

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

heavy traffic area, the periodic authentication of safety message and checking all the signatures in emergency becomes an important problem. This problem cannot be avoid completely, but it can be reduced considerably by prioritize the received messages for verification. The messages with high priority will verified often than the low prioritized one.

This new verification method based on priority has many steps to do the verification. They are as follows: first step is key initializing module where the vehicle secret key is generated and copied in the disk space of the corresponding OBU. Second is pre-processing stage. It verifies whether the emergency message correlates with the vehicle position and the current system time. If it matches, then the session parameter is generated by using the current system time and the corresponding area location by the authorized entity and a signer. Third step is signature generation from which the signature of the emergency message is generated. Finally the receiver verifies the source node and the received message's integrity. This cross layer verification scheme uses MAC layer traffic class and traffic intensity for better verification of emergency messages.

m) Secured multi message authentication protocol

The VANET always have issue of communication overhead and delay in message authentication, since the trusted authority provides anonymous certificates and distribute secret keys to all the OBUs. To solve this issue, the Secured Multi Message Authentication Protocol (C.SelvaLakshmi, et al., 2013) is implemented in the VANET network which makes the OBU in the network to update its certificate periodically. This protocol intakes the batch verification technique which overcome the processing of message authentication.

The protocol starts with the usual initialization process as the vehicle register its identity to the Trusted Authority TA and the signature id is generated by using the DSA algorithm. TA provides and saves the parameters to each vehicle. The parameters are certificate, timestamp, secret key, and shared public key. Message authentication is done using two steps namely message broadcasting and message verification. These steps include the process of exchanging the shared public key, revocation check calculation, message integrity verification and etc. The next step of the protocol is based on the RSU which is a fixed infrastructure on the road side. Every OBU belong to the RSU should their certificate to the TA through the available RSU. In this protocol, the RSU do this verification instead to TA and sends the update to the TA in secure manner. This results in reduced communication overhead and minimized delay of message authentication. The protocol introduces the batch verification technique which uses the Secure Hash Algorithm (SHA) to enable verification of group messages simultaneously. Finally the revocation process is done for the making the revoked certificates into non-revoked for spreading the safety messages without ignoring.

n) Authentication framework with privacy preservation for VANET

The most common issues in the VANET are privacy and security issues. The paper (Huang Lu, et al., 2012) presents a Novel ID Based Authentication Framework with Adaptive Privacy Preservation for VANET where in the pseudonyms are generated by its own and it is used as a identifiers and two different schemes are used for authentication process. This frame is best suited for providing privacy preservation between vehicles. The proposed protocol has the protocol initialization step where the RTA request the vehicle id of the vehicle based on the hash value. Privacy preserving authentication is done for the vehicle to RSU and RSU to vehicle.

Many IBS and IBOOS schemes are proposed in the framework which is mainly based on the RSA and ECC signatures. Since RSA based signature in the authentication framework results in the large message size, the ECC signature is incorporated with the proposed framework form the IBS and IBOOS schemes. The authentication of V2R and R2V, the IBS is considerably taken as best scheme. Then the IBOOS scheme is efficient for the V2V authentication and the signature like ECC and DP is used frequently.

o) Strong privacy preservation using pseudonymous authentication scheme

The important problem in privacy preserving is the distributed certificate service when the RSU is considered as a certificate issuer. Providing centralized certificate issuers is another problem therefore the RSU itself act as a sub certificate issuer. This also becomes a problem if the RSU is being attacked by the attackers in the network. This leads to know the pseudonymous certificates publicly. When this process increases, then number of fault RSU leads to the easy tracing of vehicle location. To overcome this problem, the proposed an Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation (Yipin Sun, et al., 2010), named PASS is introduced.

This protocol comprises of four steps. First step is to develop a novel scheme where in the pseudo identities of the pseudonymous certificate are generated. The CRL size in the PASS protocol is linear by revoking the revoked user's unexpired certificates. Second step is certificate updating scheme where in the RSU issue the pseudonymous certificate and the PASS makes the vehicle to store such large set of certificates. This reduces the overhead in the communication. Third step is providing strong privacy preservation to the vehicles. Because the RSU just issue the certificate but it do not know any information regarding the certificate. Hence it is easy for

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

the adversaries to trace the vehicle location and cause serious damage. Finally, simulation results in that the proposed scheme has attain different advantages such as reduce the overhead in updating the certificate, authentication overhead and revocation overhead in the vehicular network.

4. CONCLUSIONS

Many approaches and methods for achieving the privacy and the authentication in the VANET environment are being the recent research. Some of the protocols and methods are reviewed in this paper. All these methods and protocols are having both advantages and disadvantages. Hence a perfect mechanism is yet to be proposed to overcome all the disadvantages of these protocols and methods. The research on VANET implementation will not get succeed until the security and privacy is achieved.

REFERENCES

Hu Xiong, Jianbin Hu, Tao Yang, Wei Xin, Zhong Chen. 2012. Efficient Privacy-Preserving Authentication Protocol for Vehicular Communications with Trustworthy. Journal Security and Communication Networks. 5(12): 1441-1451.

Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho and Xuemin (Sherman) Shen. 2008. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. Conference on Computer Communication, IEEE, 0743-166X, 13-18.

Zuowen Tan. 2010. A Privacy-Preserving Mutual Authentication Protocol for Vehicle Ad Hoc Networks. Journal of Convergence Information Technology. 5(7).

Mahalakshmi. R.S and Alangudi Balaji. N. 2014. Privacy Preserving Authentication for Security in VANET. International Journal of Advanced Research in Computer Science and Technology. 2(1), ISSN: 2347-9817.

Jianhong Zhang, Yuanbo Cui and Zhipeng Chen. 2012. SPA: Self-certified PKC-based Privacy-preserving Authentication Protocol for Vehicular Ad Hoc Networks. International Journal of Security and Its Applications. 6(2).

Bharati Mishra, Saroj Kumar Panigrahy, Tarini Charan Tripathy, Debasish Jena, and Sanjay Kumar Jena. 2011. A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation. World Congress on Information and Communication Technologies 11-14, Mumbai, India.

M. Ramya and N. Mohanapriya. 2014. Quick Message Authentication Protocol for Vehicular AD HOC. International Journal of Emerging Technology and Advanced Engineering. 4(4), ISSN 2250-2459.

Lei Zhang, Qianhong Wu, Bo Qin and Josep Domingo-Ferrer. 2011. APPA: Aggregate Privacy-Preserving Authentication in Vehicular Ad Hoc Networks. Lecturer Notes in Computer Science, Series Volume: 7001, Series ISSN: 0302-9743, pp. 293-308.

Xuedan Jia, Xiaopeng Yuan, Lixia Meng and Liangmin Wang. 2013. EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication. Journal of Software. 8(8).

Surabhi Mahajan and Alka Jindal. 2010. Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks. International Journal of Computer Applications, ISSN: 0975-8887, 1(20).

Sapna S. Kaushik. 2013. Review of Different Approaches for Privacy Scheme in VANETs. International Journal of Advances in Engineering and Technology. 5(2): 356-363, ISSN: 2231-1963.

J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos and J. - P. Hubaux. 2007. Mix zones for location privacy in vehicular networks. In: Proc. International Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia.

L.Huang, K. Matsuura, H. Yamane, and K. Sezaki. 2005. Enhancing wireless location privacy using silent period. In Proc. IEEE WCNC. pp. 1187- 1192.

X. Lin, X. Sun, P.-H. Ho and X. Shen. 2007. GSIS: a secure and privacy preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. 56(6): 3442-3456.

K. Sampigethava, L.Huang, M.Li, R.Poovendran, K.Matsuura and K.Sezaki. 2007. AMOEBA: Robust location privacy scheme for VANET. In IEEE J. Sel. Areas Commun. 25(8): 1569-1589.

2011. Conditional Privacy through Ring Signature in Vehicular Ad-hoc Networks Brijesh Kumar Chaurasia and Shekhar Verma M.L. Gavrilova and C.J.K. Tan (Eds.) Trans. on Comput. Sci. XIII, LNCS 6750, pp. 147-156, 2011 © Springer-Verlag Berlin Heidelberg.

Subir Biswas and Jelena Misic. 2013. A Cross-layer Approach to Privacy-preserving Authentication in WAVE-

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

enabled VANETs. IEEE Transactions on Vehicular Technology. 62(5): 2182-2192, ISSN: 0018-9545.

C. SelvaLakshmi, N. Senthil Madasamy, T. Pandiarajan. 2013. Secured Multi Message Authentication Protocol for Vehicular Communication. International Journal of Advanced Research in Computer and Communication Engineering. 2(12), ISSN: 2319-5940.

Huang Lu, Jie Li, Mohsen Guizani. 2012. A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs. Conference on Computing, Communication and Applications, IEEE, pp. 345-350, ISSN: 4577-1717, 11-13.

Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen and Jinshu Su. 2010. An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular. IEEE Transactions on Vehicular Technology. 50(7): 3589-3603, ISSN: 0018-9545.