A Survey on various Security Mechanisms used in Vehicular Ad-hoc Networks

Dr. A.Ranichitra[1], Dr. V.Lakshmi Praba[2]
[1]*Sri S.R.N.M.College, Sattur,India,*
[2] *Rani Anna Govt College for Women, Tirunelveli,India.*
[1] *ranichitra117@gmail.com*
[2]*vlakshmipraba@rediffmail.com*

***Abstract*— Recent developments in wireless communication technologies led to the evolution of Vehicular Ad hoc Network (VANET). The main goal of VANET is to afford communication between vehicles without negotiating security. Adding security to VANET environment is challenging due to the unique features of the network, such as Dynamic topology, Mobility modelling and prediction of the vehicles. Though security in VANET is a significant challenge to face, identification and isolation of malicious vehicles are very important. It is obvious that any malicious vehicle altering or generating replay attack of the critical messages could be ruinous to the other trusted vehicles. Security Mechanism is a process designed to detect, prevent or recover the communicating entities from various security attacks. This paper discusses the various asymmetric cryptography security mechanisms and its applicability in various secure routing protocols of VANET.**

***Index Terms*— VANET, Security, attacks, adversaries, Public-Key Cryptography, Key Management, digital signatures.**

I. INTRODUCTION

Vehicular Ad-hoc Network has emerged as an important research area over the last few years. VANETS have now been established as reliable networks that vehicles use for communication purpose on highways or urban environments. Along with the benefits, there arise a large number of challenges in VANET such as provisioning of QoS, high bandwidth connectivity, security and privacy. The need for a robust VANET is strongly dependent on its security. The challenges of security must be considered during the design of VANET's architecture, security protocols, cryptographic algorithms, etc. To find out the most wanted area of research in VANET, the major survey papers related to VANET design issues, various protocols and algorithms were reviewed.

From the survey it is observed that several protocols have been proposed for Vehicular Ad-hoc Networks. Most of the protocols focus on problems related to routing information. As more applications were developed to take advantage of the unique properties of VANET, it soon became obvious that security of routing information has to be addressed. A security mechanism against the basic security services like authentication, confidentiality, integrity, non-repudiation and availability is needed. The protocols are also susceptible to various security attacks such as Rushing attack, Sybil attack, Black Hole attack, Wormhole attack, Blackmail attack, Replay attack and Routing table poisoning attack.

Though security in VANET is a significant challenge to face, most of the research has been focused only on designing architectures, routing protocols and various applications including broadcasting of warning messages and entertainment applications of VANET. The information related to life safety is very vital so that the information should not be altered by an attacker. Major survey on various security mechanisms used in VANET are reviewed in [1,2,3].

This paper is organized as follows; Section II describes the types of attackers. Section III describes adversaries in VANET. In Section IV the various Security Mechanisms used in VANET and the paper is concluded in Section V.

II. TYPES OF ATTACKERS

The different types of attackers are

1. **Insider vs. Outsider**. The insider is an authenticated member of the network who can communicate with the other members. This means that he/she possesses a certified public key. The outsider is considered by the network members as an intruder.

2. **Malicious vs. Rational.** A malicious attacker seeks no personal benefits and aims to harm the members or the functionality of the network. Rational attacker seeks personal profit.

3. **Active vs. Passive**. An active attacker can generate packets or signals. A passive attacker contents himself with eavesdropping on the wireless channel.

4. **Local vs. Extended**. An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local. An extended attacker controls several entities that are scattered across the network [4].

III. ADVERSARIES IN VANET

Securing VANET is a major challenge, having a great impact on the future deployment and application of vehicular networks. Appropriate security architectures should be developed in providing secure communication between vehicles and RSUs. Moreover, behaviour of vehicles is an important issue that can intimidate the security of communication and message delivery in vehicular networks[5]. The following are some of the

attacks that may exist in the VANET communication environment.

Sybil attack: Sybil attack is defined as a malicious device illegitimately taking on multiple identities at the same time so that it can report an existence of false bottleneck [6].

Bogus message attack: The bogus message attack is a basic attack in which an attacker can diffuse a false message to affect the normal behaviour of other vehicles and to gain maximum utilization of the network usage.

Denial of Service (DoS): A DoS attack is an attack against any system component that attempts to force the nodes to halt the normal services. This type of attack aims to crab the availability of certain nodes or even the services of the entire network.

Eavesdropping: Eavesdropping or sniffing is a network layer attack which captures packets from the network which are transmitted by the other nodes and reads sensitive information.

Masquerading: In masquerading attack, an attacker acts to be another node by using false identities and can be motivated by malicious nodes [4].

Wormhole attack: In wireless networks, the wormhole attack tunnels the packets between two remote nodes and disseminate erroneous messages in the destination area [4].

Message Suppression attack: An adversary may use one or more vehicles to launch a suppression attack by selectively dropping packets from the network. An attack might also suppress congestion alerts before selecting an alternate route, which leads the nodes to wait in traffic[7].

Industrial Insiders: Attacks by insiders are particularly insidious, and the extent to which vehicular networks are vulnerable will depend on other security design decisions. For example, if mechanics can update the software on a vehicle, they also have an opportunity to load malicious programs. If one allows vehicle manufacturers to distribute keys, then a single rogue employee at one manufacturer could create keys that would be accepted by all other vehicles [7].

Access control: Access control is necessary for applications that need fine-grained definition of the rights that a user or infrastructure component has. Another form of access control can be the exclusion of misbehaving nodes (e.g. by an intrusion detection system using a trust management scheme) from the VANET by certificate revocation or other means [8].

Greedy Drivers. In a congestion avoidance system, a greedy driver might try to convince the neighbouring vehicles that there is considerable congestion ahead so that they will choose alternate routes and allow the greedy driver a clear path to his/her destination.

IV. SECURITY MECHANISMS USED IN VANET

Security Mechanism is a process designed to detect, prevent or recover the communicating entities from various security attacks. Security mechanisms can be categorized as symmetric cryptography and asymmetric cryptography security mechanism. Symmetric cryptographic techniques include AES, DES, Double DES and Triple DES. As symmetric cryptography poses the following disadvantages [9], this literature survey focuses on asymmetric cryptographic mechanisms.

- In a two party communication, the key must remain secret at both ends and the key has to be changed frequently to have a sound cryptographic practice.
- In a large network, many key pairs have to be managed and hence an effective key management technique is required.

Figure A shows the various asymmetric cryptographic mechanisms used for providing security in the networks.

The following are some of the asymmetric cryptography security mechanisms used in securing VANET environment used by various researchers in their research contributions.

A. Public-Key Cryptography

The idea of Public-Key Cryptography is to send messages in such a way that only the person who receives them can understand them even if the method of encryption is discovered by 'an enemy' who intercepts the messages.

Public-Key cryptography facilitates the following tasks:

- Encryption and decryption allow the two communicating parties to disguise information they send to each other. The sender encrypts information before sending it. The receiver decrypts the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- Tamper detection allows the recipient of information to verify that it has not been modified in transit.
- Authentication allows the recipient of information to determine its origin, that is, to confirm the sender's identity.
- Non-repudiation prevents the sender of information from claiming at a later date that the information was never sent.

Public-Key Cryptography can be achieved by the following methods:

- Public-Key Certificate
- Key Management
- Digital Signatures
- Message Authentication.

1. Public-Key certificate

Public-Key certificate is an electronic document used to prove ownership of a public key. The certificate consists

of a data part and a signature part. The data part contains clear text data including, a public key and a string identifying the party to be associated. The signature part consists of the digital signature of a Certification Authority (CA) over the data part, thereby binding the subject entity's identity to the specified public key. CA verifies the signature, and if the signature is valid, CA provides the key which will be used to communicate with the other entities. ID-Based Encryption, ECDSA, RSA are some of the techniques used to achieve Public-Key certificate from the trusted entity of the communication parties.

Zhu et al [10] introduced a novel Aggregated Emergency Message Authentication (AEMA) scheme to achieve efficient authentication on emergency events in VANET, to validate an emergency event by obtaining the public-key certificate from the Offline Security Manager (OSM) after proper registration of the vehicles. This scheme effectively addresses both the efficiency and security issues in VANET. To reduce the transmission cost, syntactic aggregation and cryptographic aggregation techniques were used and adopt batch verification technique is used for efficient emergency messages verification. In AEMA, two types of entities, namely the Offline Security Manager (OSM) and vehicles. Each and every vehicle can join the network by generating Public Key, Public-key certificates, and certificate verification. The vehicles are grouped as clusters and every node at the head of the cluster is known as the header, which is responsible for forwarding the data to the next cluster. When one or more vehicles sense an emergency event, every vehicle has to generate their Secure Emergency Reports (SER) independently. The SER has to be verified to check the validity of the certificate and the supporting signature. The cluster head which acts as an aggregator of the cluster will perform SER aggregation by aggregating multiple SERs into a single SER, and it verifies the batch signature and its certificate. The effectiveness of AEMA for defending against attack is based on the combination of the traceability property and the distributed trust mechanism. The traceability property ensures that any adversary sending multiple claims against a common event will be detected. The distributed trust mechanism guarantees that the number of the adversaries in the VANET is less than a threshold value.

Wasef et al, [11] proposed an Efficient Certificate Management scheme for Vehicular communications (ECMV) which offers a flexible interoperability between different administrative authorities and an efficient way for any On Board Units(OBU) to update its certificate anywhere anytime in a timely manner. ECMV scheme includes four levels as a hierarchical structure in which the Master Authority (MA) which is the root of the system, level 2 includes the certification authorities, level 3 is the Road Side Units and level 4 is On-board Units. In this architecture, authentication is achieved by using the ID-based cryptography for CAs and certificate-based authentication for RSUs and OBUs. The MA generates the public/secret key pairs for each CA to verify the certificate of any RSU and OBU. Each CA first signs the certificate set for each RSU in its coverage area using certificate signing keys. The second signing key is used as a partial signing key to generate secret OBU-certificate signing keys for each RSU. The public keys can be used by any entity to verify the certificate of any OBU or RSU. This scheme remarkably decreases the complexity of certificate management and achieves excellent efficiency and scalability.

Park et al [12] proposed an efficient authentication protocol with anonymous public key certificates for secure vehicular communications based on the system model issue on the fly anonymous public key certificates to vehicles by road side units. The authenticity of the vehicles and RSU is assured by checking the legitimacy of their ID-based private keys issued by the Trusted Authority [TA]. When the vehicle requests a certificate from the RSU, it decrypts the certificate to find the pseudo-id, public key and the time period and verifies the same with the revocation list received from TA. After obtaining the anonymous short time public key certificate from RSU, it can use the certificate for safety message authentication protocol. This protocol considers a key-insulated signature scheme for certifying anonymous public keys of the vehicles. This protocol is more efficient in RSU valid serving capability and message verification than group signature-based protocols.

Xiong et al [13] proposed a secure and an efficient vehicle-to-roadside communication protocol which combines the best aspects of identity-based public key cryptography approaches (implicit certification) and traditional public key infrastructure approaches. A certificate-based cryptosystem is applied here not only to preserve the implicit certificate, but also to retain the desirable properties of identity-based key management approaches without the inherent key escrow problem. The security of the proposed scheme is analyzed based on its correctness, unforgeability, prevention of replay attack and prevention of replication attack. As a certificate-based signature is generated by a valid RSU which can surely be identified by the verification procedure, correctness can be maintained. Unforgeability is obtained as RSU signs an arbitrary number of messages by guaranteeing unforgeability and data integrity.

i) ID-based encryption

ID-based encryption (or **identity-based encryption (IBE)**) is a type of public-key encryption in which the public key of a user has some unique information about the identity of the user. ID-based encryption was proposed by Adi Shamir [14]. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. The PKG first publishes a master public key and retains the corresponding **master private key**. Given the master public key, any party can compute a public key corresponding to the identity by combining the master public key with the identity value. To obtain a corresponding private key, the party is authorized to use the identity and contacts the PKG, which uses the master private key to generate the private key for identity.

Huang et al [15] proposed a new privacy preservation scheme named Pseudonymous Authentication based Conditional Privacy (PACP) scheme in which vehicles use pseudonyms instead of their true identity to obtain probably good privacy. This scheme uses the Identity-Based Encryption (IBE) for secure communication. The vehicle that uses PACP scheme registers with motor vehicle department using its identity and gets a ticket. It uses the ticket to communicate with an RSU in its neighbourhood to obtain tokens. Then the vehicle uses the token to generate the pseudonyms. The pseudonyms are known only to the vehicles, not to the other entities in the network. The vehicles in the network interact with roadside units to help them generate pseudonyms for anonymous communications. This scheme also provides an efficient revocation mechanism that allows malicious vehicles to be identified and revoked from the network, and also it is reported that the scheme is efficient in computation and storage.

ii) ECDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). ECDSA was first proposed in 1992 by Scott Vanstone[15]. The key generated by the implementation is highly secured, and it consumes lesser bandwidth because of small key size used by the elliptic curves. Significantly smaller parameters can be used in ECDSA than in the other competitive systems such as RSA and DSA, but with equivalent levels of security. Some benefits of having smaller key size include faster computation time and reduction in processing power, storage space and bandwidth.

Zhang et al [17] proposed a novel road side unit RSU-aided message authentication (RAISE) in which RSU is responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. RAISE adopts the k-anonymity property for preserving the privacy of the user. To authenticate the message's sender and guarantee the message's integrity, OBUs or RSUs should sign with their private key transmission by introducing an efficient batch signature verification scheme for communications between vehicles and RSUs. ECDSA signature has to be attached for each Inter Vehicle Communications (IVC) messages before they are sent. The RSUs can verify multiple received signatures at the same time so that the total verification time can be dramatically reduced. In RSU-aided message authentication (RAISE) scheme, the vehicle tries to associate with detected nearby RSU and gets the symmetric secret key and a pseudo ID. The RAISE scheme has many advantages because of its lower computation and communication overhead. RAISE also protects the vehicles privacy by adopting the k-anonymity approach. In addition, a cooperative message authentication scheme named COMET has been introduced that works in the absence of RSU. COMET not only efficiently reduces the message loss rate but it is also resilient against the misbehaviour of vehicles.

2. Key Management

Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. A keying relationship is the state wherein communicating entities share common data (keying material) to facilitate cryptography techniques. This data may include public or secret keys, initialization values, and additional non-secret parameters.

Key management encompasses techniques and procedures supporting

1. Initialization of system users within a domain;
2. Generation, distribution and installation of keying material;
3. Controlling the use of keying material;
4. Update, revocation, and destruction of keying material and
5. Storage, backup/recovery, and archival of keying material.

The objective of key management is to maintain keying relationships and keying material in a manner which counters relevant threats such as

1. Compromise of confidentiality of secret keys.
2. Compromise of authenticity of secret or public keys. Authenticity requirements include knowledge or verifiability of the true identity of the party a key is shared or associated with.
3. Unauthorized use of secret or public keys. Key Management includes group key management and Certificate revocation.

Lu et al [18] introduced an Efficient Conditional Privacy Preservation (ECPP) protocol based on-the-fly short time anonymous key generation between an OBU and an RSU. This protocol also addresses the issue on anonymous authentication for safety messages with authority traceability. This scheme focuses on the two security issues, efficient safety message, anonymous authentication and efficient tracking of the source of a disputed safety message. To achieve authentication, anonymity and unlinkability, three levels of user privacy has been defined. When an RSU or OBU submits its identity for registration, TA returns the system parameters and private key. RSU issues a short time anonymous key generation when an OBU passes the RSU request for it with its pseudo-id where anonymity can be achieved. This protocol has been evaluated in terms of the OBU anonymous key storage and computation overhead for an OBU to verify a valid safety message and computational complexity of the TA for tracking a safety message. ECPP protocol is not only capable of providing the conditional privacy preservation that is critically demanded in the VANET applications, but also is able to improve efficiency in terms of the minimized anonymous keys storage at each OBU, fast verification on safety messages and an efficient conditional privacy tracking mechanism.

i) Group key management

Group Key Management means managing the keys in a group communication. Most of the group communications use multicast communication so that if the message is sent once by the sender, it will be received by all the users. The main problem in multicast group communication is its security. In order to improve the security, various keys are given to the users. Using the keys, the users can encrypt their messages and send them secretly.

Chim et al [19] proposed two secure and privacy enhancing communication schemes for VANETs to handle ad-hoc messages and group messages for Inter-vehicle communications with the help of software based solutions for security and privacy preservation which makes use of only two shared secrets to satisfy the privacy requirement. This scheme allows the RSU to perform the signature verification process. This model proposed a group communication protocol to allow known vehicles to form a group for secure communications. Each vehicle in the group stores all the group public keys and the decrypted Common Group Secret (CGS) values. RSU does not know CGS since TA encrypts it using its shared secret with each vehicle. When a vehicle sends a group message including the Group Public Key (GPK), it generates its pseudo identity and signature. GPK used by the receiving vehicles knows which group public key is used for verification. This protocol completes within the coverage area of RSU. Individual vehicles just cannot communicate on those sections of roads without RSUs, but the vehicles in the same group can communicate without the help of RSU. This scheme gives lower message overhead and higher success rates.

ii) Certificate Revocation

When a certificate is issued, it is expected to be in use for its entire validity period. However under various circumstances, the certificate may become invalid prior to the expiration of the validity period. Such circumstances include change of name, change of association between subject and CA and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA needs to revoke the certificate.

Sun et al [20] proposed an efficient Pseudonymous Authentication Scheme with Strong privacy preservation (PASS) for secure vehicular communications. In this scheme, the size of the certificate revocation list is linear with the number of revoked vehicles. PASS supports Roadside Units-aided distributed certificate service that allows the vehicles to update certificates while moving. Certificate Revocation list not only satisfies the security and privacy requirements of VANET but also significantly reduces the revocation cost and the certificate updating overhead. It also provides strong privacy preservation to the vehicles so that the adversaries cannot trace the legitimate vehicles even though they have compromised all RSUs.

Wasef et al [21] presented several security mechanisms to complement the PKI services for privacy, efficient authentication and revocation, and have also proposed a mechanism for efficiently mitigating the effect of a DOS attack. In this model, location privacy is achieved by using Random Encryption Periods (REPs) [22], where a vehicle changing its certificate surrounds itself with an encrypted communication zone using group communications until it ensures that all the conditions to be tracked are violated. Only unrevoked vehicles in this zone can decrypt the communication using the shared group key. In this way an outsider attacker will not be able to capture the messages broadcast by the vehicles as the outsider attacker does not have the group key.

This model has an Efficient Decentralized Revocation (EDR) protocol for VANETs, which enables a group of neighbouring vehicles to completely revoke a nearby misbehaving vehicle. The EDR protocol is based on a secret sharing scheme, where a master secret key is divided mathematically into a number of shadows, and the shadows are probabilistically distributed to all the vehicles. When a vehicle misbehaves, one of its neighbouring vehicles acts as a revocation coordinator and sends a revocation of the misbehaving vehicle request to the neighbouring vehicles. Each of the neighbouring vehicles uses its shadow to calculate a revocation share and forwards it to the revocation coordinator.

Every vehicle keeps track of all invalid signatures received at a particular time period and if the ratio of the number of invalid signatures and the total number of received messages reaches a threshold value, then the vehicle starts to sign the outgoing messages using HMAC which is calculated using the group key. On receiving the messages, the vehicles compare the HMAC value with the calculated values. If there is a match, it continues signing, otherwise it drops the messages. DoS attacks have slight effect on the authentication delay which can mitigate the effect of DoS attack, and appending HMAC to the messages enables the vehicles to more quickly detect and drop the invalid signatures.

3. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient to believe that the message was created by a known sender, so that the sender cannot deny having sent the message and that the message was not altered in transit. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature. The concept of digital signature was introduced in 1976 by Diffie and Hellman [23].

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key from a set of possible private keys and provides a private key and a corresponding public key.
- A signing algorithm that produces a signature.

- A signature verifying algorithm that accepts or rejects the message on receiving the message, public key and a signature.

The various types of digital signatures include Blind Signature, Group Signature and Proxy Signatures.

i) Blind Signature

Blind signature was introduced by Chaum[24] is a form of digital signature in which the content of a message is blinded before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties.

Zhang et al [25] proposed a location privacy preserving authentication scheme based on blind signature in the elliptic curve domain for Roadside unit to Vehicle Communications (RVC). This scheme not only provides fast authentication but also guarantees the security and location anonymity to the public. In this scheme, the identity of each vehicle is well protected, since the authentication credentials corresponding to a particular vehicle are blind and transparent to both server and Access Points (AP). The tracking problem of the vehicle is also removed during the handover process of the vehicle with various APs. Since mutual authentication process of the proposed scheme only requires a fast exponentiation computation instead of time-consuming pairing computation, the authentication delay has been significantly decreased in the proposed scheme.

ii) Group Signature

Chaum and van Heijst [26] introduced the concept of a group signature. A group signature has the following properties:

(i) Only Members of the group can sign messages.
(ii) Anyone can verify the validity of a signature but no one is able to identify which member of the group signed.
(iii) In case of disputes, the signature can be opened to reveal the identity of the group member who signed it.

Lin et al [27] proposed a novel secure and privacy-preserving protocol based on group signature and identity-based signature techniques. This protocol not only guarantees the requirements of security and privacy but it also provides desired traceability of each vehicle. This model used digital signature technique to sign every message sent by the RSUs and OBUs which can be verified by the receiver and ensure that the integrity and authenticity of the messages along with the no-repudiation property. The security mechanism can be divided into the following categories as the security between two OBUs and between OBU and RSU. The security between the OBUs is obtained by using a list of anonymous certificates for message authentication which are stored in the Transportation Regulation Center (TRC). They proposed a security protocol by using the group signature scheme to sign the messages sent by the vehicles.

The group signature techniques reduce the workload of the public key verification and certificate path verification operations. The communication between RSU and OBU is obtained using the identifier string of each RSU as the public key to sign the messages from RSUs whereas license plate numbers are used as the public keys of OBUs. With the group signature scheme, security, privacy and efficient traceability are achieved without inducing the overhead of managing a huge number of stored certificates at Membership Manager and Tracing Manager sides. Further, the complexity involved in managing public key and certificate can be minimized. This model demonstrates that the delay and loss rate can be reduced even in the presence of a large computational latency incurred due to the cryptographic computations.

Hao et al., [28] proposed a novel distributed key management scheme for group signature-based VANETs. This considerably facilitates the revocation of malicious vehicles, location privacy protection, heterogeneous security policies and maintenance of the system. In this scheme, RSU will be responsible for distributing group private keys in a localized manner, the vehicles are the users and the authority is the tracer. The vehicles get group private key dynamically from the RSU which controls the area where the vehicle enters. If there is a dispute, the signature will be reported to the authority. The authority uses the key and signature to retrieve the vehicle's group private key and identifies the vehicle. Even though RSUs are key distributors they are semi-trusted as they may be compromised. These compromised RSUs may collude with the malicious vehicles. This protocol prevents compromised RSUs and malicious vehicles from attacking the network.

iii) Proxy Signature

The notion of proxy signature was first introduced by Mambo et al in 1996. A proxy signature scheme is an important investigation in the field of digital signature which involves three entities: an original signer, a proxy signer and a verifier. It provides tools to the original signer to delegate his signing right to a particular signer, known as proxy signer. Once the proxy signer signed the message on behalf of the original signer, the verifier, who knows the public keys of the original and proxy signers, verifies the validity of the proxy signature after receiving it.

Hyoung et al [29] proposed a secure and efficient protocol for a VANET environment which satisfies the requirements efficiency, privacy and traceability. This scheme adopted proxy signature cryptography to authenticate vehicles and RSUs and to delegate the RSU to issue short-lived certificates only for authenticated vehicles and also maintains revocation list on behalf of the vehicles. The basic idea is to sign messages with epidermal, anonymous and traceable identities for network security. The issue of the short- lived certificate is authorized by the trusted authority. In order to have the storage efficiently, RSU maintains the revocation list on behalf of the vehicles. This protocol significantly improved the security, privacy and efficiency of a VANET.

4. Message Authentication

Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by the sender. Any message authentication mechanism has two levels of functionality. At the lower level, a function is used to produce a value which acts as an authenticator to authenticate the message. This lower level function is then used as a base in higher level that enables the receiver to verify the authenticity of the message. This may be grouped into various classes like Hash function, Message encryption, Message authentication code, HMAC and SHA.

i) Hash Functions

A hash functions is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length called hash values. The most common cryptographic uses of hash functions are with digital signatures and for data integrity. With digital signatures, a long message is usually hashed and only hash value is signed. For data integrity, the hash value corresponding to a particular data is computed and protected. The third application of hash function is their use in protocols involving a priori commitments, including some digital signature schemes and identification protocols.

Zhou et al [30] presented a lightweight and scalable protocol P^2DAP to detect Sybil attacks. While a malicious node pretends to be multiple, the other nodes can detect it in a distributed manner through passive overhearing by a set of fixed nodes called Road Side Boxes (RSB). The detection of Sybil attacks does not require the vehicles to disclose their identity, and hence the privacy is also preserved. The proposed method distributes the computation workload from Department of Motor Vehicle (DMV) to RSBs while releasing only a limited amount of information using hash collusions. P^2DAP is expected to efficiently catch attackers with a small overhead and delay even with large number of road side attackers.

The summary of the review of literatures of the various researchers are listed in Appendix B with the security mechanisms, security attacks addressed and the observations achieved from their study.

V. CONCLUSION

Security and secure routing in Vehicular Ad-hoc networks have been of interest for quite a long time among the research community. The information related to life safety is very vital so that the information should not be altered by an attacker. The attacker that exists in the network have to be identified and isolated from the network, and hence the various secure routing protocols created based on various security mechanisms are discussed in this paper. Each and every scheme has its own advantages and disadvantages. In future, a secure routing protocol may be created which suit the unique characteristics of vehicular network and addresses the various possible attacks that are addressed in this paper.

REFERENCES

[1] Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. Communications Surveys & Tutorials, IEEE, 10(4), 78-93.

[2] Mishra, B., Nayak, P., Behera, S., & Jena, D. (2011, February). Security in vehicular adhoc networks: a survey. In Proceedings of the 2011 International Conference on Communication, Computing & Security (pp. 590-595). ACM.

[3] Gillani, S., Shahzad, F., Qayyum, A., & Mehmood, R. (2013). A survey on security in vehicular ad hoc networks. In Communication Technologies for Vehicles (pp. 59-74). Springer Berlin Heidelberg.

[4] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks." Journal of Computer Security 15.1 (2007): 39-68.

[5] Praba, V. L., & Ranichitra, A. (2013, April). Isolating malicious vehicles and avoiding collision between vehicles in VANET. In *Communications and Signal Processing (ICCSP), 2013 International Conference on* (pp. 811-815). IEEE

[6] Fuestes J.M, Gonazalez-TablasA.I,Ribagorda A, "Overview of Security Issues in Vehicular Ad-hoc Networks" Handbook of Research on Mobility and Computing, 2010.

[7] Parno, Bryan, and Adrian Perrig. "Challenges in securing vehicular networks." Workshop on hot topics in networks (HotNets-IV). 2005.

[8] Kargl, Frank, Zhendong Ma, and Elmar Schoch. "Security engineering for vanets." Proc. 4th Wksp. Embedded Sec. in Cars (2006): 15-22.

[9] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2010). Handbook of applied cryptography. CRC press.

[10] Zhu, H., Lin, X., Lu, R., Ho, P. H., & Shen, X. (2008, May). AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad-hoc networks. In Communications, 2008. ICC'08. IEEE International Conference on (pp. 1436-1440). IEEE

[11] Wasef, A., Jiang, Y., & Shen, X. (2008, November). ECMV: efficient certificate management scheme for vehicular networks. In Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE (pp. 1-5). IEEE.

[12] Park, Y., Sur, C., Jung, C. D., & Rhee, K. H. (2010). An Efficient Anonymous Authentication Protocol for Secure Vehicular Communications. J. Inf. Sci. Eng., 26(3), 785-800.

[13] Xiong, H., Qin, Z., & Li, F. (2010). Secure vehicle-to-roadside communication protocol using certificate-based cryptosystem. IETE Technical Review, 27(3), 214.

[14] Shamir, A. (1985, January). Identity-based cryptosystems and signature schemes. In Advances in cryptology (pp. 47-53). Springer Berlin Heidelberg.

[15] Huang, D., Misra, S., Verma, M., & Xue, G. (2011). PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. Intelligent Transportation Systems, IEEE Transactions on, 12(3), 736-746.

[16] S. Vanstone, "Responses to NIST's Proposal", Communications of the ACM, **3**5, July 1992, 50-52.

[17] Zhang, C., Lin, X., Lu, R., Ho, P. H., & Shen, X. (2008). An efficient message authentication scheme for vehicular communications. Vehicular Technology, IEEE Transactions on, 57(6), 3357-3368.

[18] Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2008, April). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE (pp. 1229-1237). IEEE.

[19] Chim, T. W., Yiu, S. M., Hui, L. C., & Li, V. O. (2011). SPECS: Secure and privacy enhancing communications schemes for VANETs. Elsevier:Ad-hoc Networks, 9(2), 189-203.

[20] Sun, Y., Lu, R., Lin, X., Shen, X., & Su, J. (2010). An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. Vehicular Technology, IEEE Transactions on, 59(7), 3589-3603.

[21] Wasef, A., Lu, R., Lin, X., & Shen, X. (2010). Complementing public key infrastructure to secure vehicular ad-hoc networks [security and privacy in emerging wireless networks]. Wireless Communications, IEEE, 17(5), 22-28.

[22] A. Wasef and X. Shen, "REP: Location Privacy for VANETs using Random Encryption Periods," ACM Mobile Net. Apps., vol. 15, no. 1, 2010, pp. 172–85

[23] Diffie, W., & Hellman, M. E. (1976, June). Multiuser cryptographic techniques. In Proceedings of the June 7-10, 1976, national computer conference and exposition (pp. 109-112). ACM.

[24] Chaum, David. "Blind signature system." In Advances in cryptology, pp. 153-153. Springer US, 1984.

[25] Zhang, C., Liu, R., Ho, P. H., & Chen, A. (2008, March). A location privacy preserving authentication scheme in vehicular networks. In Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE (pp. 2543-2548).

[26] Chaum, D., & Van Heyst, E. (1991, January). Group signatures. In Advances in Cryptology—EUROCRYPT'91 (pp. 257-265). Springer Berlin Heidelberg.

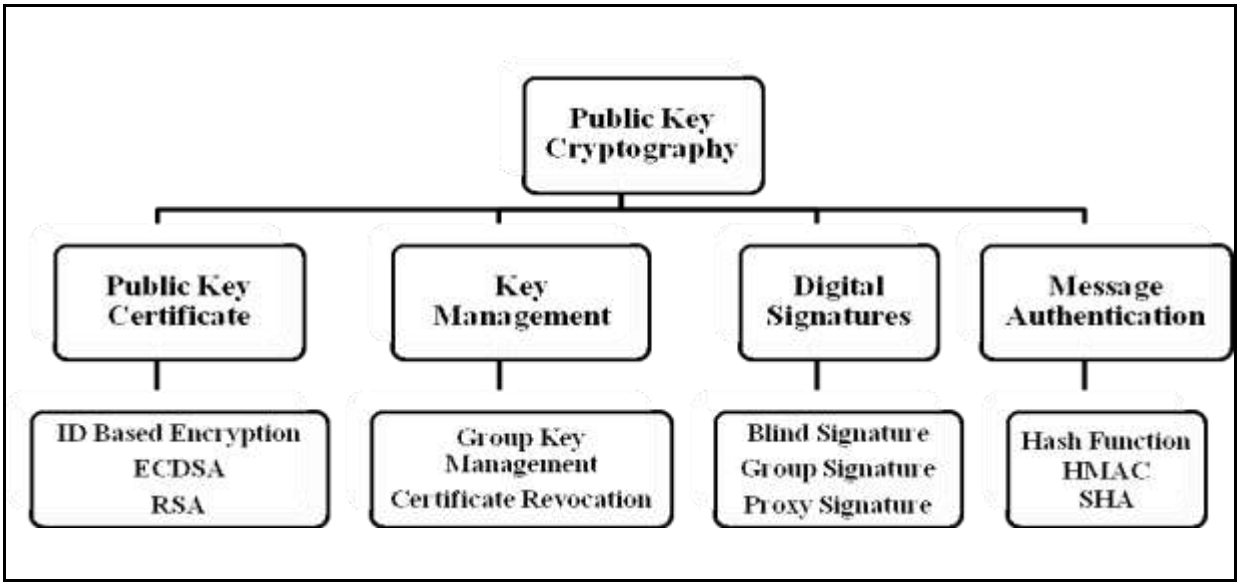
[27] Lin, Xiaodong, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. "GSIS: a secure and privacy-preserving protocol for vehicular communications." Vehicular Technology, IEEE Transactions on 56, no. 6 (2007): 3442-3456.

[28] Hao, Y., Cheng, Y., & Ren, K. (2008, November). Distributed key management with protection against RSU compromise in group signature based VANETs. In Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE (pp. 1-5). IEEE.

[29] Hyoung-Kee, C., In-Hwan, K., & Jae-Chern, Y. (2010). Secure and efficient protocol for vehicular ad-hoc network with privacy preservation. EURASIP Journal on Wireless Communications and Networking, 2011.

[30] Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. (2011). P^{2}DAP—Sybil Attacks Detection in Vehicular Ad-hoc Networks. Selected Areas in Communications, IEEE Journal on, 29(3), 582-594.

Appendix A Asymmetric Cryptographic Security Mechanisms



Appendix B Summary of various secure routing protocols used in VANET environment.

S.No	Protocol	Security Mechanisms	Security attacks addressed	Observations
1.	AEMA[9]	Public Key Certificate	False data injection attacks Sybil attacks	Reduction of transmission attack. Reduces the computation cost with increase in secure emergency report.
2.	ECMV[10]	Public Key Certificate	Authentication	Efficient in updating certificate anywhere any time. Decreases the complexity of certificate management.
3.	EA2P[11]	Public Key Certificate	Anonymous Authentication. Vehicle Tracing	Effective Message Verification.
4.	[12]	Public Key Certificate	Authentication & Integrity. RSU ID exposure Prevention of RSU Replication.	No Key escrow Slightly expensive Reduces the communication Overhead.
5.	PACP[14]	Identity based encryption	Privacy Preservation	Efficient Computation and storage.
6.	RAISE[16]	ECDSA	Message integrity and source authentication Conditional privacy Preservation Internal attacks	Reduces computation and communication overhead. Reduces message loss rate.
7.	ECPP[17]	Key Management	Message authentication.	Reduces the key storage. Fast verification on safety messages.
8.	[18]	Group Key generation	Privacy Violation Anti traceability attack. Impersonation attack.	Reduces Message Overhead.
9.	PASS[19]	Certificate Revocation	Privacy Preservation	Reduces the revocation cost & certificate updating Overhead.
10.	EDR[20]	Certificate Revocation	DOS attacks	Protects the location Privacy of the vehicles from outsiders.
11.	[24]	Blind Signature	Identity Violation. Movement tracking Violation	Reduces the authentication delay. Protects the identity of the vehicles.
12.	GSIS[26]	Group Signature	RSU Replication attack Replay Attack	Storage space is reduced. Complexity in managing public key and certificate is reduced.
13.	[27]	Group Signature	Appropriating the ID of Other Vehicle. Receiving key without acknowledgment. Colluding with vehicles Deny of reporting.	Preventing Compromised RSUs and malicious vehicles from attacking.
14.	[28]	Proxy Signature cryptography	Privacy Preservation	Light Computational Load. Efficient Storage management.
15.	P^2DAP[29]	Hashing	Sybil Attack	Reduces Communication Overhead.

