Enhancing the Communication Efficiency with Cluster-Based and Certificate Revocation Schemes for Vehicular Adhoc Networks

Ms.Jisha Raj T
Assistant Professor,
Department of CSE,
Vidya Academy of Science and
Technology Technical Campus,
Kilimanoor, Trivandum, Kerala, India

Dr.C. Brijilal Ruban,
Professor & Head,
Department of CSE,
Vidya Academy of Science and
Technology Technical Campus,
Kilimanoor, Trivandum, Kerala,

Abstract:

The development of vehicular communication (VC) systems, crucial for transportation safety, hinges on the efficient transmission of high-rate safety messages (beaconing). Simultaneously, there exists a consensus among authorities, industry, and academia regarding the imperative to secure VC systems. Vehicular Ad-hoc Network (VANET) technology operates by clustering vehicles and facilitating data transmission from source to destination nodes. However, malicious actors can exploit VANETs by injecting harmful data between vehicles, posing significant challenges. Current transmission practices prioritize node trust values over data trustworthiness, potentially allowing the dissemination of false or malicious messages. This approach can inflate storage and interaction overheads, particularly when updating information on compromised nodes. In order to overcome this issue introduced a new technique referred to as Cluster based Secure Communication and Certificate Revocation (SCCR) Scheme for VANET. Initially the nodes (vehicles) are gathered into various clusters, Cluster Head (CH) should be selected based upon the trusty nodes. The Certificate Authority (CA) known as trusted third party is taken into account however CA is in charge of revoking and distributing the certificates that belongs to the vehicles. The information of the CRL (Certificate Revocation List) is provided onto the Certificate Authority (CA). The mobile repository namely CH preserves the accumulated measure of group of witness nodes (active nodes) and also the measure of revoked nodes ids. From the simulation result it is verified that Cluster based Secure Communication and Certificate Revocation Scheme (SCCR) shows better performance when compared to the existing works SCKD, PPREM and VSPN in terms of the delivery ratio, throughput and latency etc.

Keywords: VANET, Road Side Unit (RSU), Certificate Revocation, Cryptography.

1. Introduction

1.1 Vehicular Ad hoc networks (VANET)

Vehicular Ad-hoc Networks (VANETs) are specialized networks that enable communication among vehicles (V2V), as well as between vehicles and roadside infrastructure (V2I). These networks facilitate the exchange of information related to road conditions, traffic updates, safety warnings, and other relevant data. VANETs typically operate using wireless communication technologies, such as Wi-Fi or dedicated short-range communications (DSRC), allowing vehicles to form temporary ad-hoc networks without relying on fixed infrastructure. VANETs have significant potential to improve road safety, traffic efficiency, and overall transportation systems through real-time information sharing and collaborative applications. However, they also present challenges related to security, privacy, and network management, which must be addressed to realize their full benefits.

These qualities of VANET might play a major part in generating implementation, current protocols, and vehicular ad hoc networks. The main aim of VANET is to accomplish maximum protection among the roads. In addition, benefits on the premise of internet and location along the road have the capacity to function by VANET [1]. New methodologies among trust that relates to VANETs come across many difficulties. Thus to estimate the trust value and enhance the applications adequacy and security of the VANETs, alluded to the past research accomplishments that relate to VANETs trust and attempt to build up trust patterns both in nodes and data to protect information procurement. [2].

The Road-Side Units (RSUs) will be utilized by CA in order to distribute the information regarding revocation. Regardless of the possibility that RSUs has been employed gradually with adequate density, a VANET have the capacity at various phases of maximum employment. In addition, to secure the privacy of the user, the certificates that get updated ought to be unknown and also away from the issues of key establishment [5]. Revocation can likewise be accomplished by depending on to the constrained lifetime certificates, in which the certificates is consequently repudiated after the expiration of lifetime. Consequently, VANETs can't exclusively rely upon the certificates with limited lifetime as a vehicle with misbehaving behavior can hurt different vehicles till the termination of its certificates lifetime [6, 7].

In this paper, introduced Cluster based Secure Communication and Certificate Revocation Scheme for VANET. The Cluster Head (CH) should be chosen from the cluster. Certificate Authority (CA) is in charge of revoking and distributing the certificates that belong to the vehicles. The information of the CRL (Certificate Revocation List) is provided onto the Certificate Authority (CA). The CA accumulates the set of revoked identities of nodes into a single value with an accumulator namely universal. The accumulator in turn checks for the nonmembership witness and for witness nodes i.e., proofs that a certificate not overridden its validity period. The CA, in turn, updates the accumulator by eliminating and adding revoked nodes and also this gets reflected with each and every CH maintaining a duplicate copy of it. After obtaining the details from CH, if it identifies valid certificate the secure transmission of messages takes place by the application of symmetric cryptography approach, where the encryption and decryption of certificates may occur.

The contribution of this paper is as follows:

- Here presented a Cluster-based Secure Communication and Certificate Revocation Scheme in order to improve the trustworthiness of the message.
- The nodes with its trust measure lesser than the least trust level are included in the Certificate Revocation List (CRL).
- Secure transmission of messages takes place by the application of symmetric cryptography approach, where the encryption and decryption of certificates may occur.
- Hereby we will evaluate the simulation results of the proposed approach, analyzed and contrasted the outcomes together with the similar as well as with the existing approaches.

Rest of this paper is sorted out as takes after. Segment 2 relates our work with existing works. Proposed arrangements of this paper are portrayed in area 3. Consequences of our work are talked about in segment 4. This paper is finished up with area 5.

2. Review of Related works

A few examinations have been carried out in clustering based certificate revocation scheme. The authors of those work showed that their analysis behind existing works was productive one.

Gannon *et al.* [9] have proposed a Privacy Preserving Revocation Mechanism (PPREM) in view of a one-way universal accumulator. PPREM gives authenticated, succinct, explicit and life-changing data about the status of revocation certificate at the time of safeguarding the clients' privacy. These works when compared with the proposed work it was verified that the proposed work was an effective one in terms of secure transmission.

Jie Zhang *et al.* [10] have introduced message transmissions trust dependent system and assessment onto vehicular ad hoc systems in which group of sharing information in regards to the condition of road or security. Moreover, the pattern of trust related information transmission pattern gathers and engenders peers' suppositions in a productive, efficient and secure route by progressively managing the scattering data. These work when compared with the existing work it was verified that proposed work delivered more outcomes in data preservation and transmission than the Ant colony routing approach.

T.W. Chim *et al.* [11] have proposed the constant road criteria to evaluate the best path and in the meantime, it should appropriately verify information source. Additionally, to ensure the driver's privacy, the query, as well as the query issued by the driver, was guaranteed by a trusted third party. These existing approaches when compared with the proposed work, the computation complexity was more due to the evaluation of best path and because of road traffic issues.

Ziwei Ren *et al.* [12] have proposed an identification approach equipped for perceiving positions of malicious nodes into the beacon message. Besides by detecting beacon message direction which has been received their neighborhood would be effectively partitioned into two sets. Moreover, consolidated together with three malevolent node identification strategies, nodes should proficiently nodes which are malicious around them in the wake of trading neighbors that gets grouped together with others data. The identification of malicious nodes turns to be a tedious process in these existing approaches.

3. Secure communication and Certificate Revocation Approach

3.1 Overview

This paper presents the Cluster-based Secure Communication and Certificate Revocation Scheme (SCCR) tailored for VANETs. Initially, vehicles (nodes) are organized into clusters, with Cluster Heads (CH) chosen based on the trustworthiness of nodes. Selection of the CH involves prioritizing nodes based on both their proximity and their level of trust. The role of the CH is to aggregate information from cluster members, ensuring that only messages trusted by the entire cluster are transmitted. This validation process enhances the overall trustworthiness of the exchanged messages within the cluster.

The Certificate Authority (CA) known as trusted third party is taken into account however CA is in charge of revoking and distributing the certificates that belong to the vehicles. The CA, in turn, broadcast the details of the certificates to the intermediate nodes commonly known as Road Side Units (RSU). This broadcasted detail is then transferred to each and every CH that is located in its scope. Thus fake key or certificates transmission among the nodes can attack the nodes. The avoidance of attacked node may lose its certificate still it contains the validity. The criteria should be followed to pick the revoked nodes from the cluster and this attacked (revoked) node is preserved in Certificate Revocation List (CRL). The nodes with its trust measure lesser than the least trust level (attacked nodes) are included to the Certificate Revocation List (CRL). The revoked nodes identities are accumulated by CA and get converted into single value with an accumulator namely universal accumulator. A Certificate Authority (CA) may sometimes revoke the attacked nodes with its certificates before their expiration dates. Here every CH functions as like mobile repository preserve the accumulated measure of a group of witness nodes (active nodes) and also the measure of revoked nodes ids.

If any of the cluster members needs any information regarding its certificate it can request CH. The accumulator, in turn, is upgraded to CA just by eliminating and adding nodes that are revoked as well as gets reflected each CH handling a duplicate of it. After obtaining the details from CH, if it identifies valid certificate the secure transmission of messages takes place by the application of symmetric cryptography approach, where the encryption and decryption of certificates may occur. Figure 1 depicts the block diagram of our proposed method.

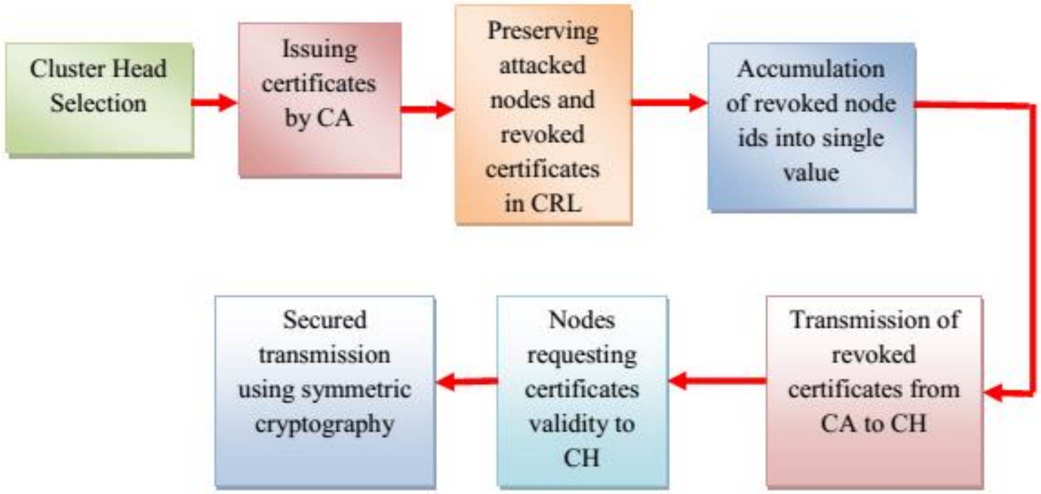
Cluster Head Selection
Issuing certificates by CA
Preserving attacked nodes and revoked certificates in CRL
Accumulation of revoked node ids into single value
Transmission of revoked certificates from CA to CH
Nodes requesting certificates validity to CH
Secured transmission using symmetric cryptography

Figure 1: Block diagram of the proposed method

3.2. Cluster Creation

In the process of Clustering nodes like mobile devices, sensors, vehicles etc. are grouped together in their geographical vicinity according to some rules. Clusters are a virtual groups. Each cluster has at least one cluster head (CH) that is selected by other cluster nodes (CN). Usually each CN has a chance to become a CH but depending on the preposition used in the algorithms one become CH. For example network connectivity, the types of nodes, (cluster relay) are used for CH selection. The size of the cluster varies from one cluster to another depending on the transmission range of the wireless communication device that a node uses. In some algorithms filters are used to prevent the nodes to join a cluster. The most frequently used filter is direction filter in which a node cannot become CN in a cluster whose CH moves in its opposite direction. Any CN can communicate directly with its CH and can communicate with other CN either directly or via their CH (either in 1-hop or n-hop). The important goal of the clustering algorithm is to achieve cluster stability. It is used as a measure of performance by the clustering algorithm. Cluster stability can be measured by frequency of CH changes or number of a CN changing its CH. The stability of clusters can be improved by selecting the CH and cluster nodes.

3.2.1 Cluster Head Selection

The cluster head can be selected from the cluster group. The entire cluster head is interlinked to one another thus for efficient correspondence as restricted resources of energy are available. In cluster based architecture the Cluster Head (CH) is in charge to establish an interaction among the cluster nodes. The vehicles are generated into various clusters and CH should be selected from the trusted nodes [1]. It means the node which is at minimum distance and the node which maintains maximum trust degree will be selected as CH. Fig.2 depicts the cluster head selection from the cluster members.

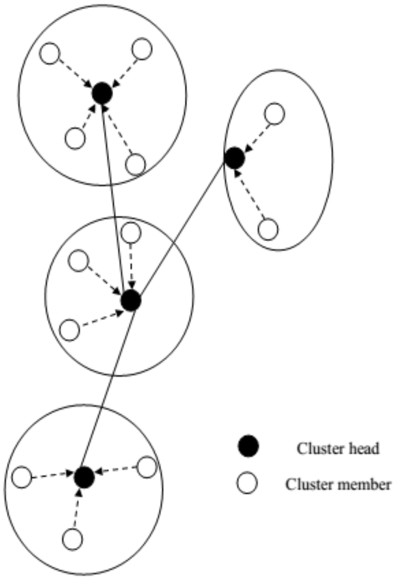

Figure 2: Representation of Cluster Head

Moreover CH determination incorporates the upcoming strides. Fig.2 illustrates the flow diagram of cluster head selection methods with the threshold.

- Initially, establishes the threshold measure and just the nodes have the capacity to function as the CH whose esteem is maximum than the established threshold measure.
- The next step is to estimate the nodes energy level and the maximum trust degree node will be selected as the CH [16].
- After the selection of CH, the counter time should be maintained to the node to remain stable as the CH to a particular period of time.
- If the first node replenishes the established time, next greatest energy level over the nodes is validated and the following node with most extreme energy level must be chosen as the CH.
- On the time if the new node is established in between the process for this the nodes energy level must be measured and contrasted together with the particular threshold value.

3.3 Issuing Certificates by CA:

The entities behind this function are as follows:

3.3.1 Certification Authorities:

CAs is in charge of producing the group of certificates. They are likewise in charge of dealing with the revocation data and allowing it to access the residual entities. The CA ought to be considered completely trusted by the entire entities of the network, so it ought to be accepted that it can't be traded off by any assailant.

3.3.2 Road-Side Units: RSU units will function as clusters intermediate node. The details of the certificates are communicated to the Road Side Units (RSU) with the help of CA; this gets transmitted to every CH that belongs to its scope. RSUs are the stable entities which might completely manage by the CA. RSUs has the ability to receive CA at whatever time since they are situated on the foundation side that does not experience the loss of links. In the event that the CA takes into account the RSU and also it is revoked by CA.

3.3.3Vehicles: The clients in the network are referred to as vehicles. They plays a major part in the cryptographic approaches [17].

3.4 Process of Revoking the Certificates Using CRL

The CA just after distributing the certificates towards the nodes, the entrance of malicious certificates may destroy the nodes. The node that gets malfunctioned combined with its certificates is stored in the list known as Certificate Revocation List (CRL).

3.4.1 Certificate Revocation List (CRL)

A Certificate Revocation List (CRL) is termed as a digital certificate list which might be revoked from the Certificate Authority (CA). The certificate distribution from CA should not exceed their expiration date as well this could not be trusted any longer. This likewise preserves the nodes that get attacked together with its certificates. CRLs are one of the sorts of blacklists that are utilized by different Web browsers, including endpoints, to validate the trustworthiness of the provided certificates.

The Certificate Revocation List (CRL) maintains a certificates list which is being revoked. Certificate Authority (CA) maintains the CRL list. Certificate Authority signs the certificates and issues the signed certificate likewise it provides the guarantee for the certificate owner’s identity. The criteria should be followed to pick the revoked nodes from the cluster and this attacked (revoked) node is preserved in Certificate Revocation List (CRL). The nodes with its trust measure lesser than the least trust level (attacked nodes) are included to the Certificate Revocation List (CRL).

At the time of certificate validation, bilinear matching is utilized. If the repository ranges $ri \in R$ the membership witness $wi \in G2$ of ri is defined to the accumulated measure $ACC(R)$ and also the measure wi proving the validation of membership function $wi^{(ci+s)} = ACC(R)$. The group element is g^{ui}.

3.5 CH acting as Mobile Repository (Mobile repositories creation):

Related to the affinity measure, a few vehicles should be chosen in order to function as a mobile repository. Thus to function as mobile repository, vehicles simply takes off the appropriately revoked data that is updated from any of the Road Side Units (RSU) (or else it can be selected from any of its repositories in its scope) and it is established to different vehicles with the accumulated measure that is signed by the CA and the information important to ascertain its witnesses. Every CH functions as like mobile repository preserve the accumulated measure of a group of witness nodes (active nodes) and also the measure of revoked nodes ids. The Mobile Repository (MR) has the capacity to establish revoked data and also it replies to the queries related to the update of the witness. Hence the revocation administration, as well as privacy of the users, is maximized. If any one of the vehicles is in demand to transfer the message, then the vehicle request CH for the certificates validity, hence the CH functions as a mobile repository.

3.6 Secure communication

The function of symmetric cryptography mechanism is to provide the secured transfer of messages, this occurs after identifying the valid certificate from the details of CH. Here the process of decryption and encryption of keys (certificates) will occur. Each and every CH situated inside the region of CA gains a key (certificate) pair of cluster head that relates to the CA's neighbor cluster. With the help of interaction between Cluster Heads (CHs), the destination can be identified. Alight the destination vehicle might be situated into similar cluster carrying the vehicle V1 otherwise the destination can be located into cluster isolated from vehicle V1, in turn, the vehicle V1 ought to discover its V2 (destination) just before the initialization of communication and prefers the appropriate approach in view of the destinations location. Based upon the function of symmetrical encryption the encryption function can be selected. Example for this is Advanced Encryption Standard (AES) [2]. The cluster member's privacy can be effectively preserved at the time of communication between vehicles. The interaction related to the destination ought to be separated into two classes: correspondence in between 2 vehicles situated in a similar cluster, and correspondence between 2 vehicles situated in 2 distinctive clusters.

Thus based upon these classifications, the approaches behind security are partitioned into two distinctive classes that will be clarified under segments 3.6.1 and 3.6.2. In addition, HMAC has been utilized as a part of a request to confirm data authentication and data integrity. Take note of that thus before transmitting information message from the vehicle V1 onto vehicle V2, the session key ought to be produced between vehicleV1and vehicleV2.

3.6.1 Correspondence between 2 Vehicles Situated in Similar Cluster

The data messages that ought to be traded along the vehicle V1, vehicle V2 and Cluster Head (CH) keeping in mind the end goal to create keys. The variables expressed in the accompanying equations are as follows, the currently generated vehicle combines with the cluster, the public or private key proxy pair combines $(y_{pvi} \| \sigma_{pvi})$ ought to be allocated to it. For this reason, CH has been termed as intermediary (proxy) that creates a Warrant Message, WV, thus in terms of vehicle V that comprises the identities (IDV) related to the CH and also to the cluster member V.

Stride 1: The Random number (R1) is picked up by the V1 node and timestamp T1 is generated. T1 parameter is one of the integer number utilized to validate the gained message of key generation. A while later, V1in turn encrypts $T1, WV1, R1, IDV2, IDV1$ key generation messages towards the pair of intermediary public/private key and directs the encrypted message on to the Cluster Head (CH).

$$H(y_{pv1} \| \sigma_{pv1}) \oplus (T1, WV1, R1, IDV2, IDV1) \tag{1}$$

Here H is referred to as Hash function, $\oplus$ demonstrates xor function, and || denotes the concatenation function. The XOR encryption ought to be a non-complex symmetric cipher which can be utilized as a part of numerous applications, in which security doesn’t characterize prerequisite. As it were, XOR is valuable towards security related algorithms, as well as for another mechanism here the data security doesn’t relate to the fundamental issues.

Stride 2: The message of received key generation is decrypted by the node CH through key pair of proxy V1's public/private and validates WV1andIDV2 to guarantee whether the vehicle V1and to the vehicle V2 are considered as eligible to convey with each other, i.e,

$$H(y_{pv1} \| \sigma_{pv1}) \oplus (T1, WV1, R1, IDV2, IDV1) \oplus H(y_{pv1} \| \sigma_{pv1}) = T1, WV1, R1, IDV2, IDV1 \qquad (2)$$

If the vehicle V1identifies authorization in order to transmit the key generation message, the random number Rh is generated by CH and also the timestamp T2 to such an extent that $T2 = T1 + 2$. At that point, CH encrypted by $IDV1, R1, T1, T2, Rh$ utilizing proxies of vehicle V2's public/private key pair and then it is transmitted to vehicle V2. Something else, a key generation message demanded by V1's to transmit will be eradicated.

$$H(y_{pv2} | \sigma_{pv2}) \oplus (IDV1, R1, T1, T2, Rh) \qquad (3)$$

Stride3: The key generation message is decrypted by the Node V2 utilizing its pair of intermediary public/private key and validates the key generation messages timestamp by

$$H(y_{pv2} | \sigma_{pv2}) \oplus (IDV1, R1, T1, T2, Rh) \oplus H(y_{pv2|} \| \sigma_{pv2}) = IDV1, R1, T1, T2, Rh) \qquad (4)$$

If $T2 = T1 + 2$ is captured, V2 eliminates its interaction. Else, V2 generates R2 the random number and produces a timestamp T3 with the end goal that T3=T2+ 1 and after that figures $HMACKT(Rh \| R2 \| R1)$, where transitory key KT is equivalent to $H(R1)$. V2 transmits the key generation message towards CH adding $(IDV1, IDV2, T3, Rh, R2, HMACKT(Rh \| R2 \| R1))$ then it is encrypted towards KT with the help of

$$EKT(IDV1, IDV2, T3, HMACKT(Rh \| R2 \| R1), Rh, R2)) \qquad (5)$$

Stride 4: The key generation message is decrypted by the node CH and validates the T3 validity. On the off chance that $T3 = T2 + 1$ is captured, TimestampT4 is generated by CH so that $T4 = T1 + 1$and it is transmitted to vehicle v1 after encrypting the key generation message.

$$EKT(IDV1, IDV2, T4, HMACKT(Rh \| R2 \| R1), R2, Rh)) \qquad (6)$$

Stride 5: V1node ascertains KT as well as decodes the key generation message which is being received and after that validates the timestamp. In the event that$T1 + 1 = T4$ is not valid, V1 eliminates the correspondence. Something else, V1 measures $HMACKT(Rh \| R1 \| R2)$. In the event that the computed makes $HMACKT(Rh \| R1 \| R2)$ similar gained $HMACKT(R1 \| R2 | Rh)$, after this process V1 calculates the session key in terms of $KS = H(R1 \| R2 \| Rh)$.

V1can utilizes Ks to encode the generated information message thus to transmit it to vehicle V2. In addition, vehicle V2 has the capacity to compute Ks thus to decrypt the vehicleV1 received the message. Take note of that a CH can get the Ks keys and along these lines, it can decodes entire cluster members communications. In any case, this is not an issue since from the trusted vehicles CH is selected, and its execution is constantly checked by other verifiers.

4 Results and discussions

The proposed SCCR is simulated using the simulator NS2. For about 100 nodes are assigned in this simulation. These nodes are randomly placed in the 1000m×1000m region. The initial energy of nodes is used in this simulation is 40J. Transmitting and receiving the power of each node is 0.660W and 0.395W. Table 1 shows simulation parameters of our proposed work. In this simulation, each cluster has a maximum of about 10 nodes. From the cluster group Cluster Head (CH) should be chosen from the cluster. Certificate Authority (CA) is being selected which is in charge of revoking and distributing the certificates that belong to the vehicles (nodes). From CA the certificates are issued to all nodes located in the clusters. The fake key distribution and fewer vitality nodes become as malfunctioned (attacked) nodes. The attacked node with its issued certificate is revoked in the CRL list. CRL list is maintained by CA. After validation of the attacked nodes certificate expiration date and it identifies that still the certificate has validity it is transmitted to Cluster Head (CH). The transmission of valid certificates takes place among the cluster members by capturing the required certificate details from CH, because CH acts as a mobile repository. The transmission of valid certificates (key) from the source vehicle to destination vehicle among the cluster and also communication in between the vehicles of the cluster occurs through symmetric encryption approach. Thus secure transmission is achieved to avoid the unwanted third parties to hack the certificates (Keys).

Parameter name	Value
Number of nodes	100-500
Area	1000m×1000m
Simulation time	50secs
Transmit power	0.660W
Receiving power	0.395W
Initial energy	40J
Transmission range	50m
Constant bit rate	500kbps

Table 1: Simulation parameters

4.1 Based on Rate

The rate of a network relays on the reliability of data, compression as well as the total number of nodes in the networks and also determines about the secured transmission among the nodes. Performance metrics of our proposed work is evaluated by varying the rates 100, 200, 300, 400, 500. Figure 3-5 shows the packet delay, delivery ratio, Energy, Thus our proposed work SCCR has been compared with the existing works SCKD (“Security scheme based on Clustering and Key Distribution”)[8], PPREM (“Privacy Preserving Revocation Mechanism”)[9] and VSPN (“VANET-dependent Secure and Privacy Preservation”) [11]. Figure 3 shows the delay of our proposed work. When the number of nodal rate increases in the network, packet (data) delay of the network also increases which is depicted in the graph. Compared to the existing works SCKD, PPREM and VSPN our proposed work SCCR has 21% less delay due to the proposed approaches. Figure 4 shows the delivery ratio of our proposed work SCCR. The delivery ratio is referred to as the ratio between the numbers of packets to be delivered at the respective simulation time. Delivery ratio diminishes if the nodal rate goes beyond the simulated time. The delivery ratio of our proposed work is 93% higher than the existing work. Figure 5 shows the Energy consumption of our proposed work SCCR. The consumption of energy gets increased if the rate of the node is maximized. Our proposed work SCCR shows less consumption of energy of about 35% than the existing work SCKD.

Overhead refers to adding up of extra data to the packet in order to reach the desired destination. If the nodal rate is increased the overhead in the system goes beyond the limit due to more arrival of data packets at a simultaneous time. When contrasted with the existing works SCKD, PPREM and VSPN the overhead of our proposed work is 32% less due to the non-collision of nodes (vehicles).

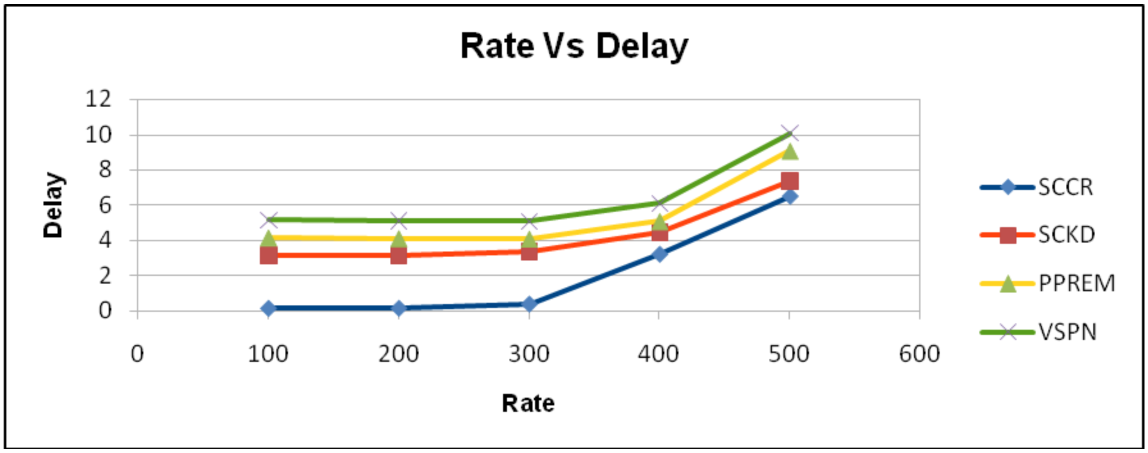

Figure 3: Rate Vs Delay

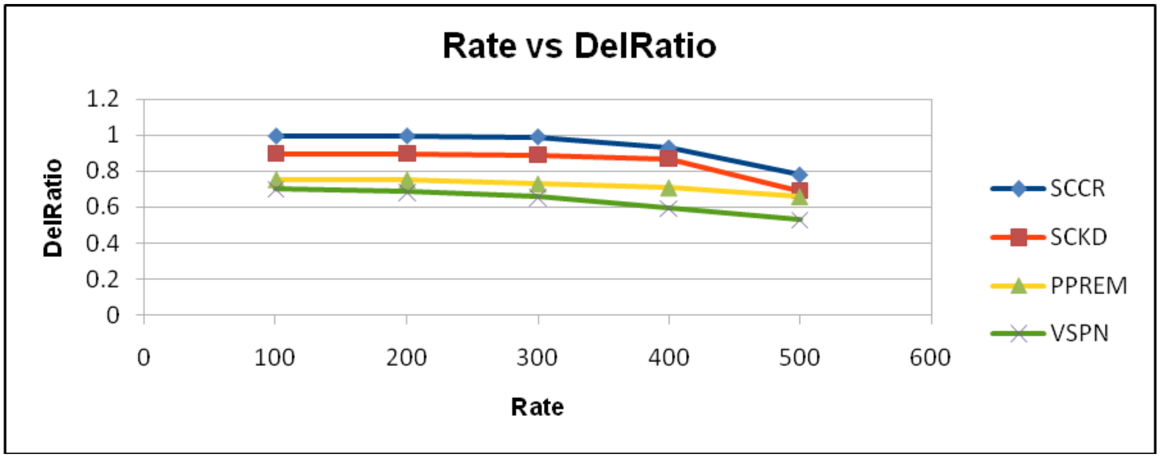

Figure 4: Rate Vs Delivery ratio

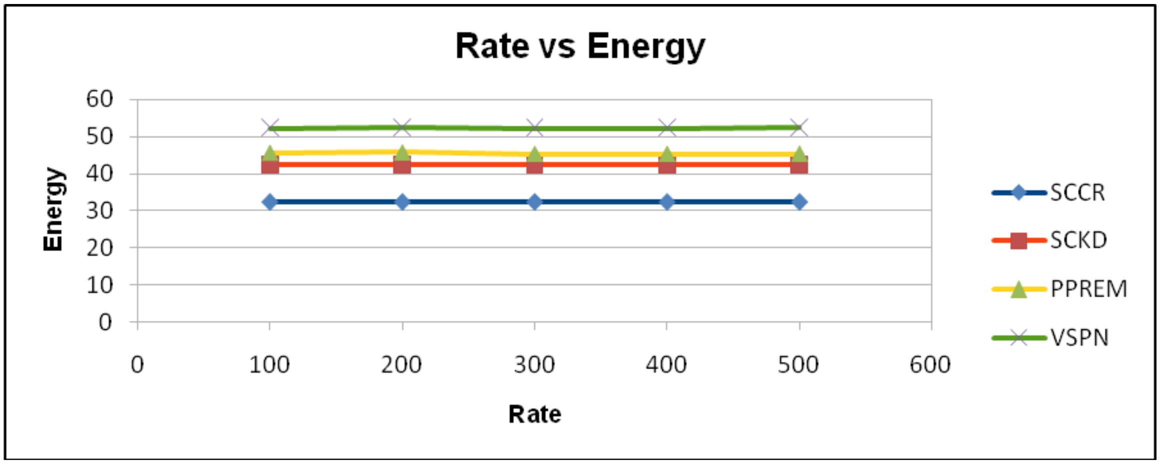

Figure 5: Rate Vs Energy

5. Conclusion

In this paper, a Cluster-based Secure Communication and Certificate Revocation Scheme for VANET have been proposed. Thus to maintain the secure communication among vehicles (nodes) symmetric cryptography approach is implemented with certificate revocation scheme. The attacked node may not lose its certificates in because CA revokes all the non-expired certificates of the attacked nodes. CA transfers it to CH holds all the details of the active nodes and also about the attacked nodes. All the cluster members can request CH to receive the details about the validity of the certificates. By this approach, unauthorized party has no ability to decrypt the transmitted valid certificate. It also resolves the communication overhead due to a limited number of attacks. The proposed method validates the trustworthiness of the nodes and also checks the trust of transmitted messages.

References

[1] Sugumar et al., Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)" Journal on Wireless Networks, pp: 1-10, 2015.

[2] Yao et al., "Using trust model to ensure reliable data acquisition in VANETs" Journal on Ad Hoc Networks, pp.232-432, 2016.

[3] Fan et al., "Cluster-based framework in vehicular ad-hoc networks", Journal on Ad-Hoc Networks and Wireless, pp.32-42, 2005.

[4] Studer et al., "Tacking together efficient authentication, revocation, and privacy in VANETs" IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1-9, IEEE, 2009.

[5] Haas et al., "Efficient certificate revocation list organization and distribution" IEEE Journal on Selected Areas in Communications, Vol.29, pp: 595-604 2011.

[6] Wasef et al., "DCS: an efficient distributed-certificate-service scheme for vehicular networks." IEEE Transactions on Vehicular Technology, Vol. 59, No. 2, pp: 533-549, 2010.

[7] Wasef, Albert et al., "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks" IEEE Transactions on Vehicular Technology, Vol. 58, No.9, pp: 5214-5224, 2009.

[8] Daeinabi et al., "An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks" Computers & Electrical Engineering, Vol.40, No.2, pp: 517-529, 2014.

[9] Gañán et al., "PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks" Journal on Computer Standards & Interfaces, Vol.36, No. 3, pp: 513-523, 2014.

[10] Zhang et al., "A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks" Vol.1, No. 4, pp: 3-15, 2010.

[11] Chim et al., "VSPN: VANET-based secure and privacy-preserving navigation" IEEE Transactions on Computers, Vol.63, No. 2, pp: 510-524, 2014.

[12] Ren et al., "Location security in geographic ad hoc routing for VANETS", International Conference on Ultra Modern Telecommunications, pp: 1-6, IEEE, 2009.

[13] Xue et al.," A trusted neighbor table based location verification for VANET Routing" Journal of Wireless Mobile and Multimedia Networks, pp: 1-5, IEEE, 2010.

[14] Sun et al., "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications", IEEE Transactions on Vehicular Technology, Vol. 59, No. 7, pp.3589-3603, 2010.

[15] Mejri et al., "Survey on VANET security challenges and possible cryptographic solutions" Journal on Vehicular Communications, Vol.1, No. 2, pp.53-66, 2014.

[16] Lin et al., "Enhancing efficiency of node compromise attacks in vehicular ad-hoc networks using connected dominating set" Journal on Mobile Networks and Applications, Vol.18, No. 6, pp: 908-922, 2013.

[17] Rivas et al., "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation" Journal of Network and Computer Applications, Vol. 34, No. 6, pp: 1942-1955, 2011.

Prof. C. Brijilal Ruban received his B.E degree from Anna University Chennai. He obtained his M.E degree in Computer Science and Engineering under Anna University. He received his Ph.D. degree in Anna University. He has published five papers in International Journal. He has more than sixteen years of teaching experience. Currently he is working as a Professor and Head of Computer Science and Engineering department, in Vidya Academy of Science and Technology Technical Campus, Kilimanoor, Trivandum, Kerala, India.