Improve Performance of Data Dissemination in VANET by Certificate Revocation List (CRL) Methodology

Tejaswita Singh
M.Tech Scholar
Electronics & Communication
Gyan Vihar University, Jaipur, Rajasthan, India
tejaswitasingh93@gmail.com

Hari Ram Tanwar
Associate Professor
Gyan Vihar University
Jaipur, Rajasthan, India
hariram.tanwar@mygyanvihar.com

***Abstract :-* The vehicular network is an exceptional example of communication to produce movement of cars for content dissemination. If we use a network coding, the vehicle will get tremendous flexibility, system stability, scalability and mobility in content sharing. Along with this, we suggested the methodology of CRL (Certificate Revocation List) to provide data secrecy. The conventional approaches are base on the encryption. The encryption further decreases the intermediate nodes co-operation that has not any expectation of file recovery. The scheme depends on obfuscation by polluting and then processing the real file. This scheme only allows informing about corrupted blocks to the intended receiver that can recover data on time. We are enhancing the rate of file download with a comparison to an earlier work algorithm. To enhance download rate performance, we are going to apply CRL (Certificate Revocation List) algorithm.**

Keywords: *Vehicular Ad-Hoc Network; Proxy-Based Authentication Scheme; Proxy Vehicle; Privacy Preservation, Key Negotiation.*

I. INTRODUCTION

The VANETs (Vehicular Ad Hoc Networks) are produced by MANETs (Mobile Ad Hoc Networks). It is the natural development of the remote network for data exchange to vehicles domain. They are the main element of ITS (Intelligent Transportation System).

In the 2000s, the VANETs were one to one application, which based on the principle of MANET. Since that time they developed research field under their rights. And by the year 2015, [1] (p3) a term VANET became identical with standard IVC. Thus the focus remains with spontaneous networking aspect. It is less with RSUs (road side units) or the cellular networks.

In current time, more voluminous road traffic influences efficiency and safety of traffic environment. Nearly, 1.2 millions of people died each year in traffic accidents. And so traffic becomes a challenging issue for traffic management. One likely way is to give traffic data to the vehicle, so the mechanism of a vehicle could understand the traffic environment. And this makes possible by exchanging data amongst vehicles. All vehicles are mobile and require the mobile network. So, that each will capable enough to operate with support infrastructure. And only because of micro electronics, it is likely to integrate network device and node into one unit with remote interconnection, that is, ad hoc network. Further, this network developed as MANET [1].

The VANET is the application of MANET. Specifically, VANET is the self-organized network which may form by the interconnecting vehicle that aims to enhance traffic management and driving safety. It is possible by accessing the internet by both drivers and programmers. The VANET provide two types of communication.

At first, real wireless ad hoc network is used in between vehicle to vehicle without the infrastructure support. The second is communication in between RSU (road side units), fixed vehicle and infrastructure. Each node is VANET and equipped with two unit types, that is, OBU (on board unit) and AU (application unit). The OBU has the capability of communication where AU performs a program by making the OBU's capability of communication. An RSU may join to network infrastructure that is joined to the Internet.[2] Fig. 1.1 describe C2C- CC VANET architecture.

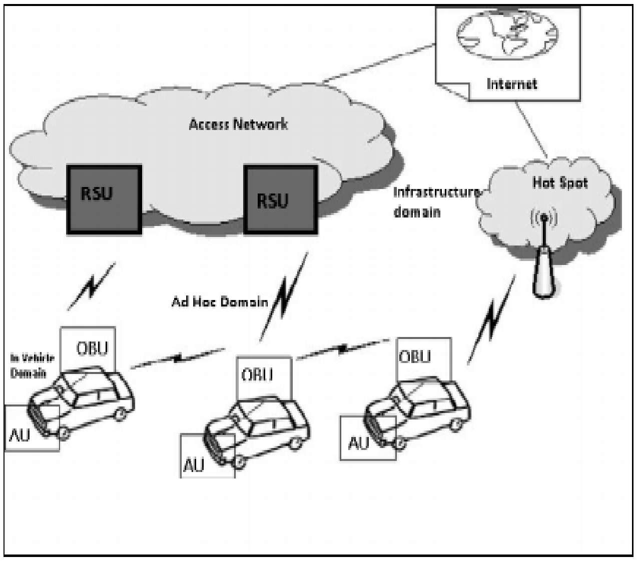

Figure 1: - The C2C- CC reference architecture [2]

The IEEE defined standard 802.11p or 802.16 (WiMax) to set up VANET. The DSRC (Dedicated Short Range Communication) has suggested that the functioning system on the band of 5.9 GHz & uses 802.11 access methods. It is standardized as the 802.11p that gives

SRC (short range communication) with the low latency. The USA allocate spectrum band of 75 MHz in the band of 5.9 GHz for DSRC. It is used by ITS (Intelligent Transportation System). And, Europe has allocated spectrum of 30 MHz in a band of 5.9 GHz for the ITS [3].

Some of the protocols may create by others too. The NOW (Network on Wheels) that correlate with CAR 2 CAR Consortium created some of the protocols. General Motors and Ford have generated CAMP (Crash Avoidance Metric Partnership) [4] to enhance VANET services. At last entire target of works concentrates on VANET service to distribute road safety information along the nodes. Hence, primary exchange of data on network signifies security role. Any successful attack may cause financial loss or lives loss. Because of this data security in VANET becomes crucial. In this thesis, we are going to discuss major attacks and security challenges on the VANET. Also, consider existing solution of such attacks.

A. VANET Applications

The arrangement of VANETS may include the commercial application. The application is where VANET could play a big role. It is further distinguish into two big categories. [3, 5]

B . Safety Related Application

These are some applications to increase safety on roads. And they are distinguishing as following:

- *Collision Avoidance:* As per some studies 60% accidents may avoid by providing the warning before an instant (half second) before to driver. [5] The timely warning message to the driver can avoid a collision.
- *Co-operative Driving:* The signal help driver by giving warnings relates to the traffic signal, lane change, etc. These signals co-operate with drivers for un-interruption & safe driving.
- *Traffic Optimization:* The traffic may optimize by signaling related to jam and accidents, etc. to vehicles. Because of this user can choose the alternate path and save his time.

C. Content Distribution Scenario And System Objective

The methodologies go for the securing the limited time distributed content to huge vehicles set which authorized for data access, as appeared in Figure 2. The essential objective is to avoid different cars to remake the parts of the original file block while it is urging them to take part actually in goals of the system so that the content at the real time may conveniently disperse. System network coding is utilized to encode information at the source and the intermediate nodes, as it turns out to be an efficient method to establish vehicular applications. As well, when cars are moving quickly and the transmission channel is getting noisy [10]. Fig.No.2 demonstrates a source that parts the blocks file and circulates linear combination to the neighboring vehicles. The intermediate nodes represented by gray cars (black cars). They have the role in encoding received packets before sending them to their particular neighbors, illustrated by white cars in Fig. 2. The vehicles are crucial to maintaining and keep up the associated topology and spread the data in between vehicles that are not in communication range. The discussion restricted to one hop and neighbors are learning the newly accessible data by checking an encoding vector before really downloading a block. The difficulty in approach is to make sure that such intermediate nodes are not able to access original file.

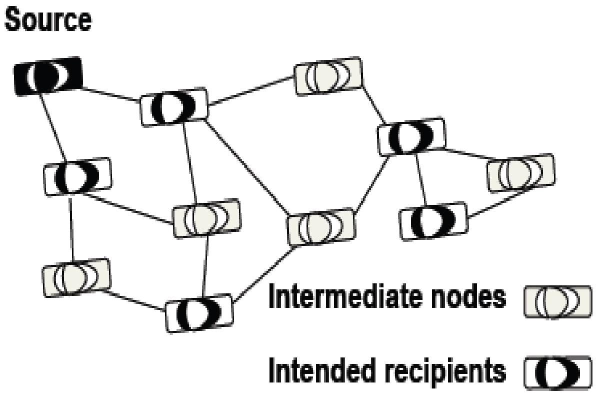

Figure 2. Content distribution network in VANET

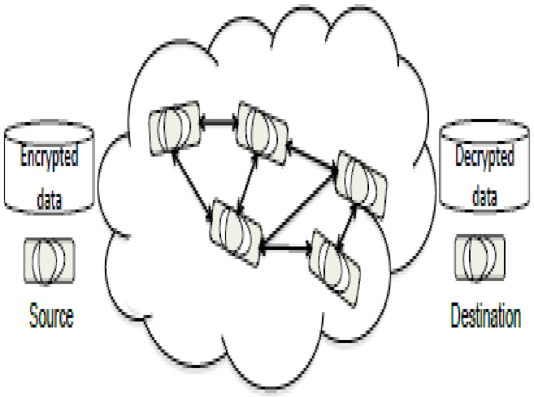

Figure 3. The source transmits encrypted content that is decrypted once the destination recovers all the blocks.

In our setting, the source utilizes a group secret key to encode information so that numerous destinations that have the same benefits can decode the content. This shared key may be circulated to the individuals by utilizing an out-band channel or at an enrollment stage if nodes subscribe to service. In conventional methodologies, depending on data encoding to secure information, at first, the source ensures file, and afterward, it utilizes random network coding to circulate an encoded blocks to a node, as appeared in Fig. No.3. Finally, the destination may decode the data when it receives effectively the ‘n’ linear independent blocks combination, where n denotes block number. In this setting, encoding stores data secrecy but an intermediate node won't care to collaborate as they have not transmitted data access and control. Along these lines, the advantage of system network coding is minimized as the vehicles have the very small probability to receive valuable data.

To the certain extent, we are applying the "winnowing and chaffing" methodology, characterized in [12], to minimize the amount of encoded data and to motivate the group of nodes to make resource contribution. The incentives comprise of their desire for data recovery. The essential thought is to pollute the content purposefully in the manner in which intermediate nodes may not recover an original file on time that may include corrupted symbols. These symbols may be distinguished and then disposed of by approved recipients as the source utilizes the safe channel to notify that file segments have been added to conceal original data. In this, we stretch that precise methodology is legitimate to secure the data that are considered for restricted time as the intermediate nodes may perform on entire file to filter out corrupted portions.

Indeed, they may attempt to discard the blocks and further check that recovered data is useful or not. The time is a function of file size and polluted blocks number. Intermediating nodes are unknown. Beginning from the particular assumption, we characterize the distinctive ways to deal with a technique to provide an efficient secrecy to weak data in a vehicular network.

D. Weak Data Secrecy

The methods which utilize for constructing blocks as- a part of our scheme of weak data secrecy are the network coding to encode the data and SRCs (Secure Random Checksums) to identify contaminated blocks. In this area, we exhibit first the SRCs role and after with detailed approach.

SRC Gkantsidis [6] has characterized the SRC. The development of SRC is as follows: The source produces ’the- components ‘m', many symbols in the block, by utilizing the secure pseudo-random generator. These elements characterized in the same finite field F2q of the network coding symbols.

E. Weak secrecy scheme (WSS)

The WSS utilizes SRCs to recognize both corrupted blocks by malicious nodes and the ones purposefully contaminated by source, as characterized in [6]. The source circulates to an approved destination substantial SRCs for those blocks which contain modified value and original content of SRCs to distinguish the contaminated content. At the point when a block received, a node computes the SRC, and if the verification fails, it utilizes a homomorphic hash capacity [6] to recognize in between encoded blocks which contaminated by source or by the intermediate nodes. In 2nd case verification of homomorphic hash fails. The intermediate nodes may recover such blocks which have not contaminated. To fortify the systems by keeping-up the same overhead amount. The source pre- processes the information before an obscurity by applying the “all-or-nothing” transformation _(x) = xM1. Where x is the information and M is an invertible matrix with the non-zero entries in limited field F2q. It is as per the suggestion of Stinson in [13] and discussed in Section II. An essential property is to apply the transformation that including an increasing complexity for an intermediate node, in order to recover the real file. Before the calculation of an inverse transform, all the corrupted blocks need to identify correctly.

In our plan, the consequence of change is conveyed in clear text by utilizing a network system coding program; though the SRCs are encoded to keep away from which unapproved clients realize that blocks get corrupted. After that, the authorized nodes get enough encrypted packets to recover an entire file, they may check the SRCs and drop those blocks which don't coordinate with their SRC values, as appeared in Fig. No. 3. At that point, the nodes get inverted all the transformation.

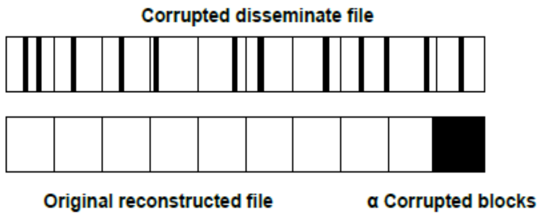

Figure 4:- . File reconstruction: a legitimate destination discards the corrupted blocks for the reconstruction of the file.

F. Public-Key Infrastructure (PKI) based Scheme

The PKI (Public Key Infrastructure) based proposal utilized for the application of vehicular signature [1], where the RSU confirms the received message one after the other. The vehicles forward messages, whenever, it will most likely be unable to be anticipated and known by RSU. What's more, this PKI-based proposal is the tedious procedures and may not fulfill the computational ability must under the dynamic traffic pattern, and because of this computational transmission overhead and complexity of RSUs increases as the vehicle quantity expanded for the validation.

Zhang et al. in [7] has suggested and presented the productive batch of the signature authentication scheme for communication amongst the RSUs and vehicles in that an RSU may confirm numerous signatures received such that the aggregate time required for authentication may mostly minimize. In the suggested scheme it is seen that an RSU may establish around 1600 messages for every second, that is not awful, but rather it is not sufficiently quick to meet the necessity of VANET confirmed speed. As indicated by the DSRC (Dedicated Short Range Communication) the convention in [8] [9], every vehicle shows the traffic safety message after each 100-300ms. It suggests the RSU must confirm around 2500- 5000 signal messages for every second if considered vehicles number should be 500 within RSU coverage. It is thought to be the incredible challenge for any existing group based scheme of the digital signature in the thesis [10] [11] [12] [13].

In vehicular communication, the messages may confirm by utilizing the ECDSA (Elliptic Curve Digital Signature Algorithm) where every signal message incorporates one certificate. A unique challenge is to figure out how to minimize the utilization of asset in transmission and calculation. All things are considered the ECDSA gives the better security; confirm authentication, non-denial yet at the same time it doesn't feature to security attacks. Another issue with the utilization of ECDSA is that it utilizes most of the costly operation, for example, scalar multiplication or the multiplication of elliptical curve point [9]. The expensive process incorporates operation of modular inversion, scalar multiplication operations. The most tedious process in ECDSA is the elliptical curve operation of scalar multiplication.

The limitations of such schemes areas:

- Message Delay
- Message Loss Rate

The VANETs Batch confirmation offers a productive technique for signature verification. The researcher Zhang et al. [7] has presented an IBV (Identity-based Batch Signature Verification) plan for the communication amongst RSUs and vehicles called as V2I (vehicular-to-infrastructure) communications, that depends on the algorithm of identity-based encoding that was suggested by the researcher Boneh. In the particular plan, the RSU may check received numerous signatures, all the while in the meantime, such that the time required for calculation may minimize significantly.

The certificate is not obliged in the verification process, because of this the transmission overhead may minimize. Contingent privacy protection can accomplish by utilizing pseudo identities and TA (Trust Authority) is capable of real identity tracing of the vehicle from its pseudo character. The researcher Zhang has upgraded the scheme of IBV is done by group testing method. The fundamental goal of utilizing such group testing is to discover invalid signatures with the negligible verification batch workload limitation by using particular scheme is:

- IBV may experience the ill effects of replay attacks.

G. Anonymous Batch Authenticated and Key Agreement (ABAKA)

The researcher Huang in [10] has suggested an ABAKA (Anonymous Batch Authenticated and Key Agreement) scheme, this plan is proposed for many value added services. The messages sent from the multiple vehicles are then session keys, and authentications are built-up in meantime. The ABAKA security plan gets resolved in the view of ECDSA. If we contrast with an essential ECDSA and ABAKA scheme, the moderately short signatures are received by the system of ABAKA, in this manner it decreases the transmission overheads and computational cost of RSUs. Later on, the work to acquire productivity and the portion of VANET's components, for example, mobility model, the predictable routing need to consider to plan novel scheme.

H. Secure and Privacy Enhancing Communications Scheme (SPECS)

The researcher Chin has presented the SPEC (Secure & Privacy Enhancing Communications Scheme), here in this plan after authentication of the batch; any vehicle may form a group with the alternative vehicles and may speak with each other safely without the RSUs. It is the ultimate plan to suggest the convention of group communication to permit vehicles to communicate securely with different vehicles in the group after authentication.

In any case, in [11], the researcher Shi-Jinn Horng has discovered that SPECS doesn’t work appropriately to imitate attacks, and a malicious vehicle may go about as a genuine entity vehicle to show fake messages or even to drive another group member to send false messages safely among themselves. The limitation of the SPECS-scheme is:

- ➢ *Impersonation Attacks*

To beat particular SPECS weakness, the researcher Shi-Jinn Horng in [11] has suggested the b-SPECS+ scheme. It fulfills diverse security needs, and weakness withstands with an impersonate attack under explicit assumption such as TA is constantly online, the repetitive TA ought to abstain from being a bottleneck or a failure of the single point. The System network model for such scheme has as appeared in fig. In future, the difficulties of VANET, for example, insider attacks can tend to avoid packet collision in between RSU and all vehicles within the range of it.

J. Conditional Privacy Preserving Authentication Scheme

The researcher Shim in [12] has proposed a scheme, here in the plan is depends on the pseudo identity-based signature. It is utilized for the secure VANET vehicle-to-infrastructure communications. The contingent protection privacy is accomplished when each message get mapped to distinct pseudo identity, and Trust power is in charge of recovering genuine character of a vehicle from pseudo-identity. The RSU confirms numerous signatures consequently by decreasing total time of verification.

The exceptional contribution is IBS (Identity-based Signature) scheme under the assumption of CDH (Computational DiffeHellman). This plan utilizes the general hash operations, rather than by using the inefficient special function known as the Map to- point function. Also, after which a safe CPAS (conditional privacy preserving authentication scheme) is built for secure V2I communications by utilizing a pseudo-IBS system to keep the balance amongst traceability and confidentiality by accomplishing the unlink ability, message integrity, traceability, anonymous authentication. The CPAS system bolsters the speediest batch process of verification check at the RSUs, such that, an ideal opportunity for time for verifying 750 signatures at the same time less than 300 ms.

Future extent of this paper will extend the difficulties to V2V communication and lead more performance evaluation on the message delay and loss ratio in the V2V communication. Additionally, the CPAS evaluation on an expansive scale of VANET test-beds with the fluctuating vehicle mobility models may conduct. In the future some VANET challenges, for example, insider attacks may tend to avoid the collusion of packets in between RSU and all the vehicles within its range.

II. PROBLEM STATEMENT

In particular research, we have found two that are mention below:

Problem 1: - We need to improve File Download Rate Vs Time. As increment in the download rate of the file increases the system speed correspondingly. Hence, it is necessary to improve downloading rate.

Problem 2: - We need to minimize elapsed time. The elapsed time is the duration of time for completing the task downloading. It is essential to reduce elapsed time as well.

III. PROPOSED METHODOLOGY

In the current research, we're working on two major problems that have mentioned in the report and specified in the problem statement. We need to enhance the downloading rate and reduce the elapsed time. To work at particular problems, we are introducing CRL (Certificate Revocation List) methodology. By that, we can improve the rate of downloading.

In the particular approach, any vehicle is receiving the message from the other vehicle take out the message and further checks for the validity of sender's certificate. If the sender has VC (valid certificate), the receiver acknowledges the message and if the sender has IC (invalid certificate) receiver ignores the message. In addition to that, the sender is not fulfilling the condition of the license; that means sender doesn't have any certificate, then the receiver will inform the RSU about the sender, and check the certificate or license whether it is correct or not. If information is correct, RSU gives the sender a VC (Valid Certificate) otherwise, RSU proceeds for IC and note down the identity of the vehicle in CRL. Refer the figure number 5 for the checking process of the signal message.

The revocation of the certificate is done when any mischievous vehicle having VC is found. Where RSU substitutes old VC with the new IC, to show that this vehicle must be maintained a strategic distance from and this happens when more than one vehicle is answering to RSU that a particular vehicle has a VC and wrong data broadcasting. See in figure 6; this report must be given to the RSU every time that any recipient gets data from the sender and finds that this data is wrong.

If the sender has a VC, then the beneficiary recipient can consider the data from the sender without fear. In any circumstances, the recipient receives several numbers of messages, where all the signal messages agree with same output result and the same data, but a particular sender sends different information, this information may consider as wrong information, on the off chance that information belongs to the same class.

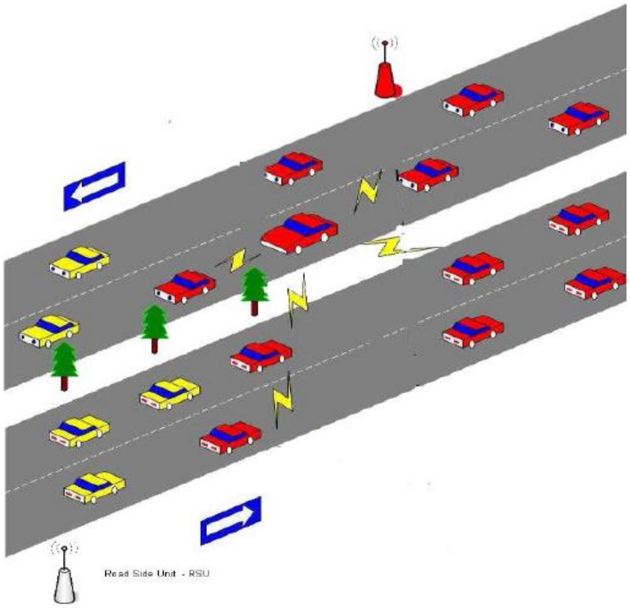

Figure 5 . Message checking procedure

Each categorization has a code, if the received signal message has the similar system off with other messages, and has the different information, and then such type of message is considered as the fake message. In particular situation the rec utilized to sends the AR (Abuse Report) for the RSU and the AR (sen Id, Message Code, Time of Receive). This statement will be forwarded to CA if RSU gets the same AR from different vehicles situated in the same range. The quantity of Report abuse messages relies on the density of traffic on the road, see figure 5.

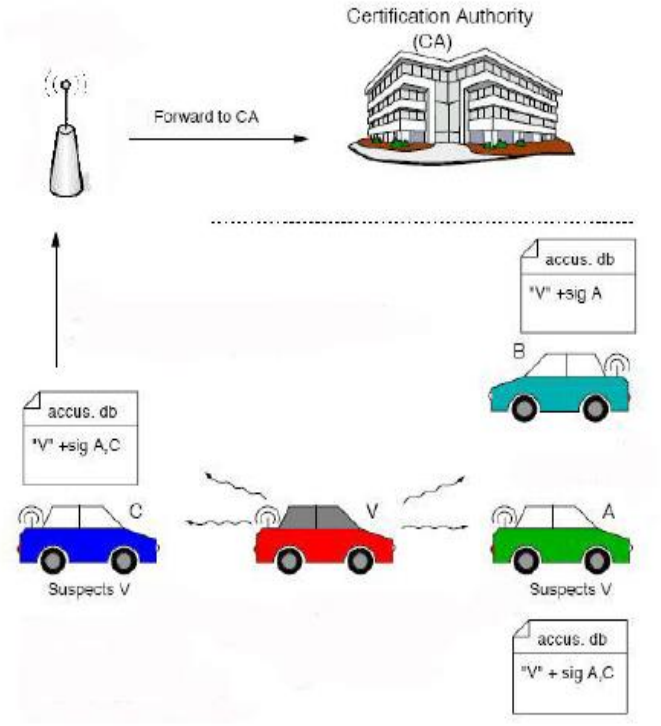

Figure 6. Certificate revocation procedure

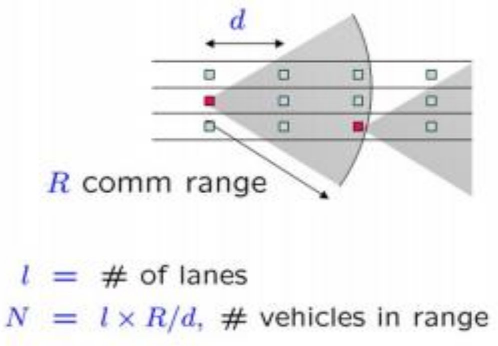

Figure 7. Calculation of the Number of Vehicles in the Range [12].

On the off chance that numerous vehicles that making the claim for a particular vehicle are close to the half of the existing vehicles, RSU will make an RR (Revocation Request) to reject the VC from the sender vehicle. Few vehicles don't create any AR since they didn't get any information from the sender vehicle (perhaps they weren't in the zone

during the broadcasting period), or have an issue on their devices, or they have an IC so that the RSU won't consider their messages. The CA makes the request of revocation to the RSU in the wake of confirming RR and redesigns CRL and after that RSU denies the VC from sender vehicle, and allocate IC for it, to show different cars in future, that this vehicle telecasts wrong information, "don't trust it." Figure No. 4.2 shows steps of certificate revocation.
Message 1: sen (sender) transmits the signal message to rec (collector), this signal message alongside electronic signature of sen, and this message further encoded with the PK (Primary Key) of rec. Any hacker can make a fictitious signal message telling rec that particular signal message originated from the sen, to stop signature being utilized.

Message 2: The rec (collector) requested to the RSU that encoded with PK of RSU and obtaining an SK for securing the connections.

Message 3: replay for the Message 2 that contains SK, sending time for the replay. The significance of time is to counteract replay attack, where the hacker (attacker) may send the particular message more than the once, with the same session key, and the same signature, so he will produce the whole connection.

Message 4: The rec sends the validity message to check whether the vehicle must maintain avoidance or not, this message has scrambled with the typical SK acquired from the RSU.

Code	Priority	Application
001	Safety of Life	Intersection Collision Warning / Avoidance
002	Safety Of Life	Cooperative Collision Warning
003	Safety	Work Zone Warning
004	Safety	Transit Vehicle Signal Priority
005	Non- Safety	Toll Collection
006	Non-Safety	Service Announcement
007	Non- Safety	Movie Download (2 hours of MPEG 1)

Table 1 :- Message Classification And Coding

Message 7: The sen transmits the signal message to rec including the VC to report for the rec (collector) in which particular vehicle must trust one. And the sending time, in here, to avoid the reply attack that happens when the hacker keeps the signal message with him and sends it after some period. It might be around then, the certificate of senders has been repudiated by RSU, so that, sen gets evaded. However, hacker tries to force the rec vehicle to trust it. After receiving data, rec checks if the signal message has the different or same information for the same category of other received message.

Message 8: if the signal message is deferent. Then the wrong information is received. The rec sends an AR (Abuse Report) for RSU that contains sen id to know that vehicle made the issue. The Message Code (MC) to know the message category, Time of Receive to find out when the signal message gets received. And the message incorporates with the Time to avoid replay attack and Signature fabrication, and the message encoded with PK of RSU.

In this circumstance, the replay attack may happen, if the hacker duplicated this message and sends it repeatedly to the RSU in several times to ensure which allegation quantity is achieved to a level, that endorsements get revoked.

In the wake of analyzing some vehicles which accused sen of sending the Invalid signal message, if the number is sensible, RSU sends the signal Message 9.

Message 9: The RSU sends the RR for CA that including Time and Serial Number to maintain a strategic distance from replay attack and Signature to evade the fabrications. The revocation Reason to state the purpose behind revocation, and sen id to identify that vehicle is problematic and the message code to identify category of message. The message then encodes with the PK of CA.

Replay assault in this circumstance happens when the hacker needs to send the same message to the CA. And by guaranteeing that particular message is from the RSU, the CA won't be able to react. And hence by bringing about for DoS attack, so RSU must utilize Serial number and Time for particular message since CA has the ton of work to do and sending a maximum number of such messages may cause the problem.

Message 10: The CA makes the Order of Revocation for RSU; this message includes SN to keep away from DoS Attack, time to avoid replay attack, the signature to evade sender Id, fabrication attack and Revocation Reason to state revocation reason.

After getting this request, the CA will update the CRL, by including the new vehicle which has been captured to the CRL and sending it for the RSU.

DoS attack may happen when the attacker continues in sending the similar message to RSU. By guaranteeing which, the message signal has started from CA. The CA message signals have the highest priority need to be prepared by the RSU, so the RSU will get an enormous amount of messages from the CA and then process it, without having secure space to communicate with different RSUs or different vehicles to avoid signature and serial number that has utilized.

Message 11: The RSU makes the repudiation (revocation), revoking VC, assigning IC, additionally particular message contains an ideal opportunity to dodge replay attack, the Signature to evade fabrication assault (attack), Revocation Reason to state revocation.

In any case, the RSU will be in charge of recharging vehicle authentications; any vehicle has an expiring certificate will communicate with the RSU to restore the license, then the RSU will check the CRL to check whether the particular vehicle has an IC or not. If there is no issue for giving another certificate for this vehicle, it can be given for a particular lifetime, when the period terminates vehicle can request CA for certificate renovation. The VC will have the unique configuration design not quite the same as the design of X.509 certificate [13] as appeared in [1].

IV. RESULTS

In this chapter , we mention the results of the existing and proposed design by CRL. we plot the three cases to show the efficiency of the weak secrecy scheme via mixing compared to the basic implementation without mixing and without network coding. In our simulation, the node average mobility is set to 10m=s, and we set p = 0:5 and q = 0:3 without loss of generality. Figure 8 clearly shows that our scheme efficiently increases the average download rate of vehicles, and in the meantime it guarantees weak secrecy protection of the data addressed to different groups. Moreover, network coding reduces drastically the download time in vehicular networks.

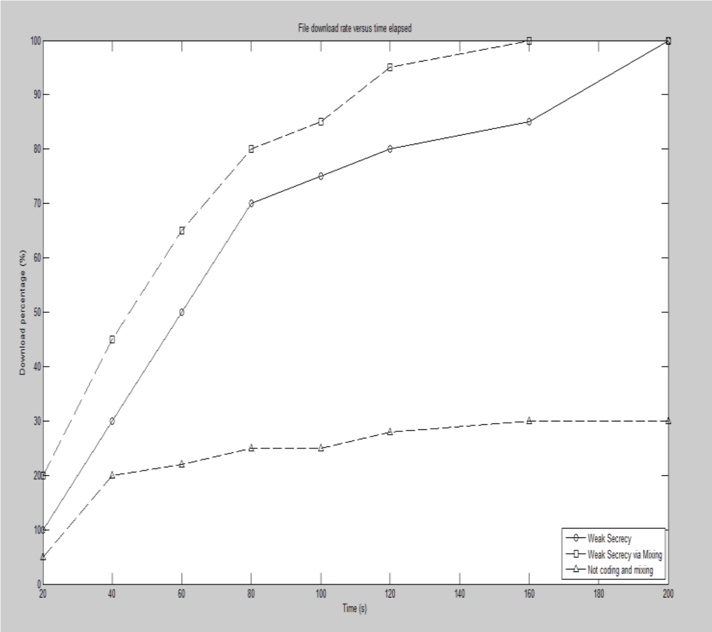

Figure 8. File download rate versus time elapsed

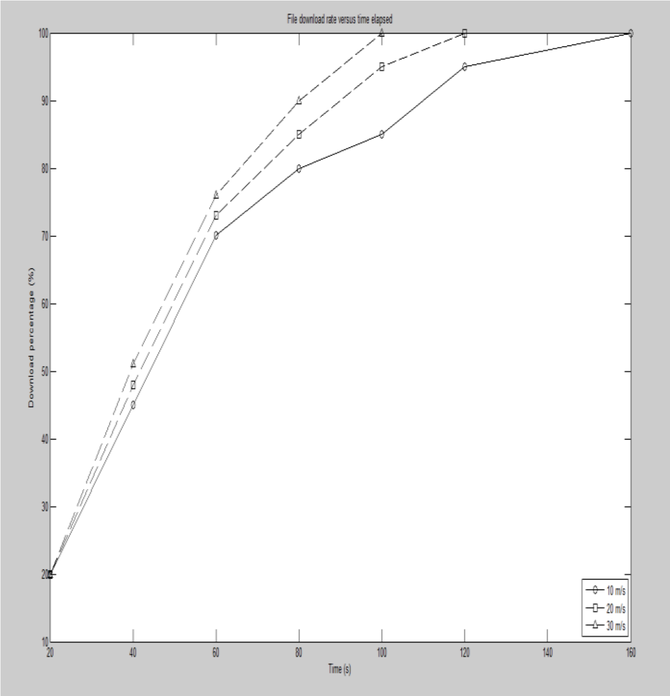

Figure 9 :-. File download rate versus simulation time with different node speed

Fig 9 is showing the file download rate versus simulation time . As we increase the downloading rate the elapsed time get reduce .

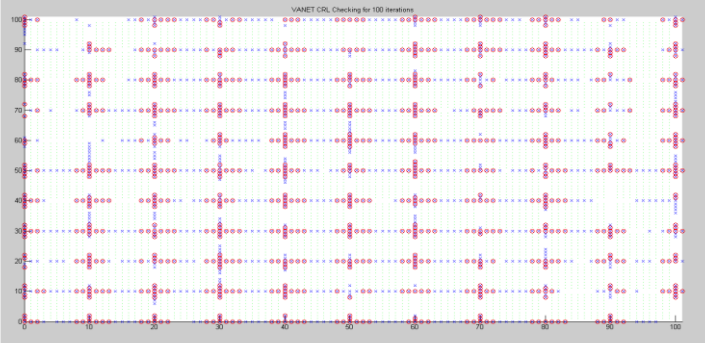

Figure 10:- VANET CRL Checking for 100 Iteration

Figure 10 is showing the VANET CRL checking for the 100 iterations . As we can see in the fig 10 the VANET CRL checking is performing for the 100 iterations .

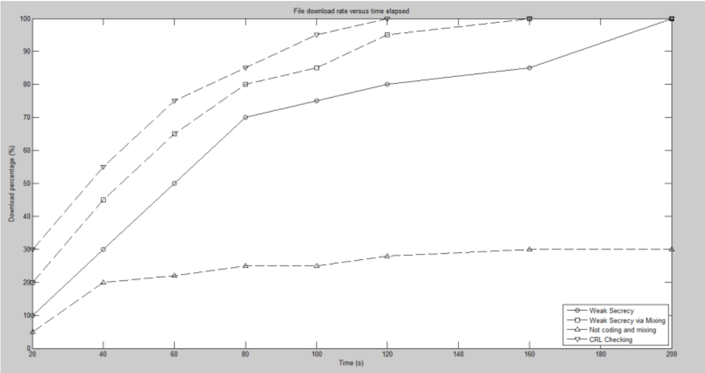

Figure 11:- File download rate for the CRL methodology

As we can see from the fig 11 by the CRL methodology we can further improve the downloading rate in the VANET n/w. From figure 11, the downloading rate graph is maximum for the proposed methodology CRL (Certificate Revocation List).

V. CONCLUSION & FUTURE SCOPE

A. Conclusion

In this research, we are exploring and working for the elapsed time and download rate of VANET network. We are performing an action to improve the download rate and to reduce elapsed time. Further, this research exhibits the novel and proficient CRL (Certificate Revocation List). It develops properties of network coding for broadcasting content in the vehicular communication systems. And it develops the approach of CRL (Certificate Revocation List) by developing an all-or-nothing implementation to remove corrupted blocks. We are discussing two conceivable ways to enhance the scheme efficiency and demonstrate that the intermediate nodes have required data to process the entire document; they cannot quickly recreate the original data. Hence, the all-or-nothing transformation has utilized to improve intermediate nodes complexity to recover the file. We can evaluate individual scheme the vehicular communication network. The simulation results demonstrate that our system has depended on mixing and obfuscation. They may help to distribute file efficiently by utilizing encryption (encoding). The scheme gives data secrecy and acquires intermediates nodes co-operation level of intermediate nodes as they have not expected consumer of content. It shows our researched system has the reasonable solution for the network coding that based on the content broadcasting in vehicular systems.

B. Future Scope

In the future for further enhance the performance of the downloading rate we can use LTE . LTE is a Long Term Evolution , which can improve the speed of the downloading system . If we apply proposed system in LTE then the performance of the downloading rate can be further increase .

References

[1] Vanetmobisim project homepage. http://vanet.eurecom.fr/.
[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. “Network Information Flow”. IEEE Transactions on Information Theory, 46(4):1204–1216, July 2000.
[3] J. Byers, J. Considine, G. Itkis, M. C. Cheng, and A. Yeung. Securing bulk content almost for free. Computer Communications, 29:280–290, 2006.
[4] M. Fiore, J. Harri, F. Filali, and C. Bonnet. Vehicular mobility simulation for vanets. In Proc. of the 40th Annual Simulation Symposium (ANSS ’07), pages 301–309, Norfolk, VA, USA, March 26-28 2007.
[5] C. Gkantsidis and P. Rodriguez. “Network Coding for Large Scale Content Distribution”. In IEEE INFOCOM, Miami, FL, USA, March 2005.
[6] C. Gkantsidis and P. Rodriguez. Cooperative security for network coding file distribution. In IEEE INFOCOM, Barcelona, Spain, April 2006.
[7] M. Jakobsson, J. P. Stern, and M. Yung. Scramble all, encrypt small. In Proc. of the 6th International Workshop on Fast Software Encryption (FSE ’99:), volume 1636 of LNCS, pages 95–111, Rome, Italy, March 24-26 1999.
[8] U. Lee, J.-S. Park, J. Yeh, G. Pau, and M. Gerla. Code torrent: content distribution using network coding in vanet. In Proc. of the 1st international workshop on Decentralized resource sharing in mobile computing and networking (MobiShare ’06), pages 1–5, Los Angeles, CA, USA, 2006.
[9] L. Lima, M. M´edard, and J. Barros. Random linear network coding: A free cipher? CoRR, abs/0705.1789, May 2007.
[10] J.-S. Park, U. Lee, S. Y. Oh, M. Gerla, and D. Lun. Emergency related video streaming in vanets using network coding. Technical report TR- 070016, UCLA Computer Science Department, 2006.
[11] R. L. Rivest. All-or-nothing encryption and the package transform. In 4th International Workshop on Fast Software Encryption (FSE), volume 1267 of LNCS, pages 210–218, Haifa, Israel, January 20-22 1997.
[12] R. L. Rivest. Chaffing and winnowing: Confidentiality without encryption. CryptoBytes (RSA Laboratories), 4(1):12–17, 1998.
[13] D. R. Stinson. Something about all or nothing (transforms). Design, Codes and Cryptography, 22(2):133–138, 2001.
[14] M. Treiber and D. Helbing. Explanation of observed features of self organization in traffic flow. arXiv, Pre-print cond-mat/9901239, January 1999.
[15] Mario Gerlay, Roberto G. Cascella_, Zhen Caoy, Bruno Crispo_ and Roberto Battiti ," An efficient weak secrecy scheme for network coding data dissemination in VANET"Computer Science Department, University of California Los Angeles, 3732F Boelter Hall, 90095, USA .