Security in VANET Through Reputation Module by Using Counter Attribute

Nikita Rathi

Computer Science & Engineering, DCE, Gurgaon

---***---

Abstract*—Now-a-days vehicle communication is becoming necessary for transmitting message about traffic and nature of the road info. Clustering is a best technique to transfer the information efficiently. But without security, it may be possible that vehicle can broadcast fake message for their bad intention or for gaining the access whole lane in a congested area. Because of this, detection of misbehaving vehicle who sent the fake message is needed. But the detection is a major challenge in present times and time consuming task also. Therefore, applying security is one of the main and important tasks to transmit message in vehicular ad-hoc network (VANET). For this purpose, we proposed new reputation system architecture with counter field to verify the authenticity of sender, semantic property of the transmitted message and also to calculate the trustier value of vehicle for checking the trustworthiness of vehicle within threshold counter value. For this objective, the digital signature on certificate is the main part to authenticate the vehicle. This paper also covers the enhancement of the revocation of all certificate of misbehavior vehicle. After describing the model in this paper, we will highlight the future work of our proposed work.*

Index Terms **-** VANET, On Board Unit (OBU), security, certificate, certificate revocation, trustworthy vehicle, misbehavior vehicle and malicious vehicle.

I. INTRODUCTION

There is a main role of transportation in everyone s life. Vehicular communication is one solution to gather the information about highway condition. Vehicular communication can be established in wired medium and wireless (ad-hoc) medium. In VANET, communication is performed by 2 types: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) and the direction of transmission information is omnidirectional. Here RSUs and CAs are commonly known as the trustworthy infrastructure components. This VANET has been proposed from the mobile ad-hoc network (MANET). But the difference between is that the speed of vehicle in VANET is higher. The VANET is described as incorporating of 3 components: vehicles: equipped with OBUs and sensors and wireless communication devices, road side units (RSUs)

: Fixed and trustier infrastructure/vehicle and third one is certification authorities (CAs): acts as government agencies that maintain record of vehicles and their drivers. It also maintains unique identity of vehicles as license plate, their secret credentials with their certificate like pseudonym set and their public/private keys.

In VANET communication, OBU of vehicle is responsible for broadcasting information about the emergency situations and traffic jams. For basic security in VANET, each OBU has an in-built authentication facility to ensure that the received data has been forwarded by a valid and authenticated vehicle. In wireless network, connections between vehicles are in very short interval of time along with its topology. This is because of very frequent moving vehicles in VANET.

In vehicular environment, standard IEEE 1609 includes 1609.1 (for resource manager), 1609.2 (for security services),

1609.3 (for networking services), 1609.4 (for lower layers) for wireless access. And the dedicated short-range communications (DSRC) protocol of 75 MHz of spectrum in the 5.9 GHz band is also used in this communication network. Here Transmission range will be approximate 1000m. But according to [10] transmission range can be changed after applying many cases.

There are multiple clustering techniques: position based technique [3], weighted based technique [10] and speed based technique [11]. By using these clustering techniques, cluster can be formed to make connectivity of network stronger and longer than that of static transmission range. In clustering, vehicles are located inside clusters and play one role from these three: cluster-head, gateway, and member of the cluster. Here if one vehicle is located within two or more clusters, it is called gateway. In this approach, each cluster has one cluster-head and one or more members (i.e. vehicles). Here vehicles those are in one cluster communicate together directly, but those are located in two different clusters communicate together via cluster-heads and gateways. Here when a vehicle moves out of its cluster, it will firstly check to itself whether it can be a member of other clusters or cluster-head. But if this vehicle finds that such other cluster exists, it can separates itself from current cluster and join to the other sufficient one. The process of joining to a new cluster is known as re-affiliation. This re-affiliation is a disadvantage of clustering techniques. Re-affiliation takes place by attacker and by fast changes in network topology in VANET.

Security is necessary to enhance transmission of the alert message in VANET. The main aim of security in VANET is to improve safety and efficiency of the transmission and channel bandwidth.

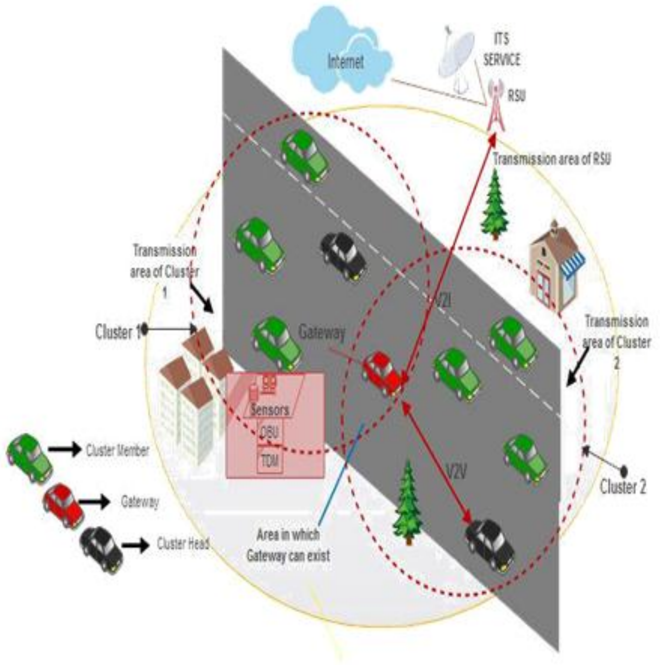

Fig. 1. VANET Model

For security, authenticity of vehicle and semantic property of transmitted message is main key. For allowing authentication, key management mechanisms is needed to build that allow sender to establish and update keys for security-sensitive operations. Here in network communication, transmitted message should be encrypted and digital signature should be applied on it by private key of sender or some other techniques like RSA algorithm. For enhancing the security, certificate and public key infrastructure (PKI) and pseudonym set will be provided by some trusted vehicle i.e. certificate authority (CA) in VANET.

Here according to [19] certificate will not have a global ID (GID) which is related to the signed vehicle. If it is, vehicle can be traced on the basis of the location of signed messages, and driver can also be tracked. Therefore, for preserving privacy, a set of anonymity (pseudonym) will be used to provide to each vehicle by certificate authority in wireless communication network.

Many techniques and algorithms have been used to secure the encrypted transmitted message. In these techniques either global id or anonymity key is provided to each vehicle by certificate authority. But in this paper, problem is occurred during examine of the trustworthiness of vehicle in ad-hoc communication network. This is happened when only one anonymity key is used for a vehicle permanently. Because of this case, location of vehicle can be tracked by non-trustworthy vehicle. In this proposed work revocation of all the certificate of non-trustworthy vehicle is done by one shared id that is given to all pseudonym set of a vehicle. This share id is same for pseudonym set of same vehicle.

A. Notation

Some notations are used in our paper. Those are:

Table I Notation

Notation	Description
^{M}mi	Message M_i of vehicle V_m
p_t	Pseudonym key t of the vehicle
pmt	p_t of vehicle V_m
TF	Trustier Field
CF	Counter Field
Enc[M_m]	Encrypted message M of vehicle m
P and Q	Prime Numbers
cm	counter value for vehicle m
C	Threshold counter value
MAC[M]	MAC algorithm is applied on message M
VM[M]	Semantic verification on message M
T V [m]	Threshold trustier value for vehicle m
tvM_{mi}	Trustier value of message M_i for vehicle m
tv[m]	trustier value of vehicle.
TVM_{mi}	Trustier value of vehicle m
N	Total number of message sent by m

II. RELATED WORK

In today s world high security and reliability are necessary in VANET communication. Therefore, security model has been proposed either to distinguish spurious messages from legitimate messages or to find the trustworthy vehicle from VANET. The requirements for VANET Security model: authentication, privacy, non-repudiation, availability, location accuracy, real-time guarantee are needed to provide security in communication network. The system that is used for authentication of messages has been also proposed to transfer authenticated messages. This system is monitored by the certificate authority. Its working is done with the help of base stations and monitoring center. This system is effective system in terms of handling security issue and also is helpful to find solution for some security issues in VANET. It is entirely cost effective solution due to the high deployment cost of the roadside situated camera.

There are two types of messages that are sent by sender: alert messages and beacon message. Beacon message is for specifying the location of the vehicles. And alert is responsible for making the sure safety of vehicles on the road. This alert message is needed to forward safety information, so that actions can be taken and vehicles can be prevented from the accidents.

In [14] one of the modular reputation system architecture has been proposed that is based on the opinion about distributed content from receiver rather than based on the behavior of sender. In this type of reputation system opinion on the trustworthiness of information is to be attached to the forwarded message before transmitting it to other nodes. After this, receivers will use this opinion as their own decision about the trustworthiness of received message. This opinion can also be observed from experience if the event is detected from partial opinions which are attached to the message.

According to [13], a distributed vehicle behavior analysis and evaluation scheme (VEBAS) have been proposed to encompass of the framework. This framework will be responsible for analyzing the behavior regarding trustworthiness of vehicle in ad-hoc network. Therefore, this scheme is also evaluating the misbehavior of vehicle and also preserves set of vehicles that cannot be analyzed because of insufficient (sensor) information.

RSU-aided certificate revocation (RCR) technique is used in [6] to perform the certificate revocation, after sender is detected as malicious. Here the relationship among three types of network entities is that CA manages the RSUs, these RSUs are connected to the internet through either wired Ethernet or wireless or any other networking technology and last one, certificate authority provides a secret key to each RSU with corresponding public key which contain the name of the RSU, the physical location, and the authorized message. In this proposed work, RSU has been signed by identity-based signature. Whenever any certificate is revoked, the CA broad-casts certificate revocation notification to all the RSUs. Then each RSU checks the status of the certificates. If certificate is confirmed as revoked, then RSU will send the warning notification to CA. Then, CA will update the all CRL list and after that, it will broadcast CRL list to neighboring vehicles and neighboring RSU of where the revoked vehicle can go. After receiving message, vehicles will update their CRLs and avoid communication with this non-trustworthy vehicle. Here movement of vehicles will be calculated based on its direction, speed and position. And CA and RSU both will be assumed as trustworthy.

A. Major Security Threats in VANET

In VANET, there are multiple security threads on which security is needed:

1) Denial of Service (DoS): DoS disturbs the communication channel and overcomes the available services from the attacker or malicious vehicles. Such that system is built useless in VANET. Some attacks which come under this thread are:

A) Flooding: The network which takes the computing resources of vehicle may be gushed by attacker. Such that genuine network traffic will be seized and channel bandwidth will be overloaded. Therefore critical information may not be forwarded to other vehicles on time.

B) Jamming Attack: This attack generates interfering transmission to prevent communication across the network channel. Here, jamming is known as low-effort exploit.

C) Broadcast Tampering/Spamming: In this attack, the hackers push modified message into the communication network. Because of this, serious problems will to be happened in traffic flows.

D) Malware: Insider attacker is introduced as mal-ware in VANET. It causes the traffic related problem having scale from congestion to accidents.

2) Routing Protocol: In routing protocol, some below attacks will be discussed.

A) Black Hole attack: In this type of attack, routers are supposed to relay packets instead of discarding it. Usually this is happened from the router which is being compromised from number of different causes.

B) Worm hole attack: In this attack, a rival receives packets at one point in the VANET, and digs them to another point in that network. After that, rival replays them from that point into the communication network. In this, tunnel is placed between two adversaries that's why this is called wormhole.

C) Gray Hole attack: This is the extension of black hole attack. In this attack, the subset of packets will be received and forwarded by receiver but sent by other one which will inject the packet. There are two types of selection:

UDP packet will be dropped by malicious vehicle whereas the TCP packet will be forwarded.

The packet will also be dropped on the basis of probabilistic distribution by malicious vehicle.

The detection of this attack is more difficult than detection of black hole attack.

3) Authentication Attacks: Through this attack attackers can generate different types of attacks like masquerading, impersonation attack, Sybil attack, replay attack, GPS spoofing.

a) Sybil Attack: In this type of attack, non-trustworthy vehicle generates the multiple false identities of many vehicles to produce an extra number of vehicles on the road. Such that non-trustworthy vehicle injects information to harm other vehicle in VANET.

b) Impersonation Attack: In impersonation attack, attacker steals the, identity of the trustworthy vehicle to illusion to receiver. For this work, attacker uses the MAC and IP spoofing into the communication network. This attack can be filtered out by broadcasting the beacon message for detecting the position of trustworthy vehicle.

B. Attacks on Privacy

Attacker can get the important information about vehicle or driver in VANET. Some attacks from those has been detailed below and also described in fig 3:

1) Identity Revealing: In this type of hacking information, attacker hacks the identity of vehicle and keeps the vehicle on risk.

2) Location Tracking: In this, attacker can track location of vehicle through its transmitted messages or global ID of vehicle during communication in network.

3) Attacks on Confidentiality: In this type of attack, attacker cans records information about vehicles and can use this info without the permissions of their owners.

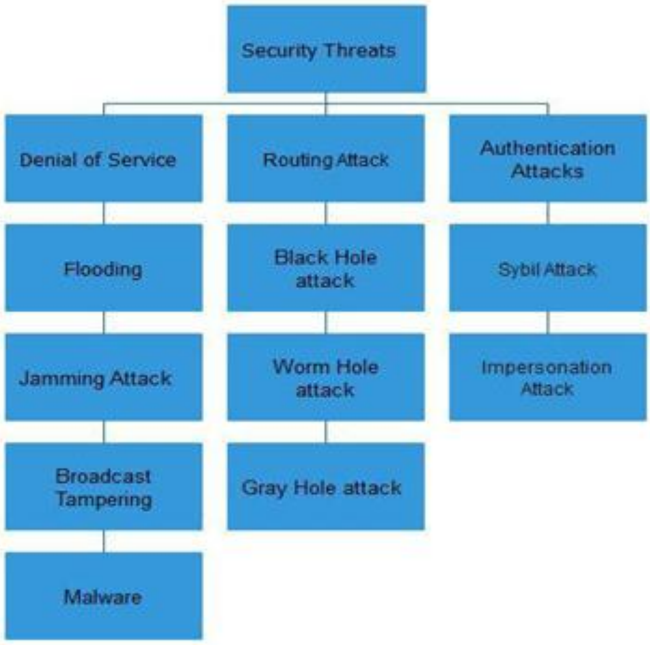

Fig. 2. Security Threats

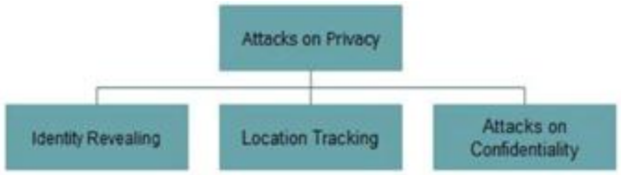

Fig. 3. Attacks on Privacy

C. VANET Security Challenges

The environment of VANET is different from the MANET s environment on the basis of high speed mobility vehicles. As described in fig 4 there are multiple security challenges in VANET.

1) Mobility: Mobility is tough to manage in VANET in comparison to that of MANET. Vehicles make the connections for very short interval of time, because of high velocity of vehicle in ad-hoc network. Therefore, communication quality will be affected due to the high mobility of vehicles.

2) Network Scalability: VANET is wide-ranging network. Such that administration of handle such a tremendous network and vehicle's security aspects are a big deal. From this, some facts are: global agencies who supervise the standard of DSRC protocol will not suitable and crucial bottleneck problem will be happened in bandwidth limitation.

3) Heterogeneity: The network is heterogeneous in VANET. This is happened because of the accessibility of the unsimilar network infrastructure in different cities.

4) Secure Positioning: There are some GPS related attacks such as signal jamming and spoofing, location attack. Due to this, GPS equipment reveals some drawback during the security. Here location can be tracked by global id that is provided to all vehicles by CA in VANET.

5) Privacy: There is a close connection between vehicles and their drivers in VANET. During security, drivers concern about revelation of their location and also their behavior. But without any security, movement of vehicle may be tracked by attackers. Therefore, financial transactions will be carried out on network communication in VANET and the privacy concern will be included in VANET.

6) Usability: Security application should be automatically configurable, i.e. vehicle s driver should not deal with any electronic system related issue.

7) Volatility: It is tough to keep the secure communication channel in VANET. Because there is long-time communication is required for securing and authentication purpose. But due to high velocity of vehicle connections cannot be established for longer period of time.

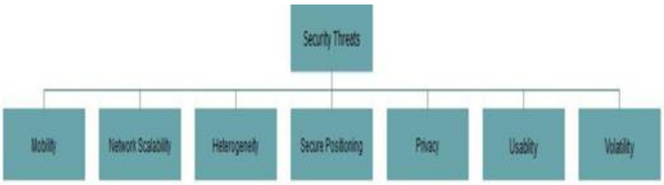

Fig. 4. Security Challenges

III. PROBLEM SOLUTION

Reputation Module: The reputation module is a system as see fig. 5. Monitoring center contains this module inside. The responsibility of this module is to check the authenticity and semantic property of message and finally to examine the trustworthiness of vehicle by calculating the trustier value of the sender vehicles as in [2]. Through this working of reputation module, non-trustworthy vehicle is to be found out in VANET communication.

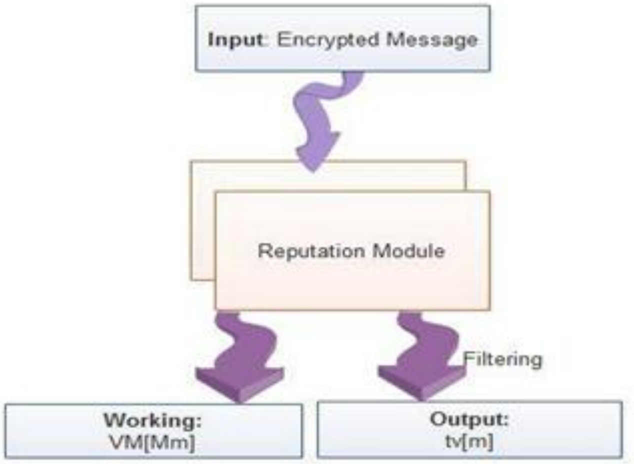

Fig. 5. Working of Reputation Module

In our proposed work, Message will be hashed for maintaining the size limit of message and then will be encrypted by RSA Algorithm. Here public key of sender will be certified by certificate authority before sending information. For security purpose, message will be signed by private key of vehicle. And for enhancing the security and reliability of channel, CA provides pseudonyms set to all vehicle for validate time interval and each pseudonym key of set will be certified by CA i.e. each vehicle will have multiple certificates with one shared id. For this work two fields: trust attribute field and counter field will be added to each certificate. And initially counter value in counter field will be assigned to 0 (zero). This all work will be done before transmitting message. After this, sender will increase the counter value by one number for increasing the time period of anonymous key. Then sender will check that the counter value is greater than or equal to threshold counter value or not. If, counter value is smaller than threshold counter value then, sender will transmit the encrypted message to monitoring center. And monitoring center will forward this message to reputation system. Here reputation module will check the authenticity and semantic property of forwarded message. And this semantic property will be checked by correctness probability of the message as defined in [2]. If message is authenticate and semantic then, trustier value of sender will be checked by this module. And this will be done on the basis of semantic property of message as describe in [2]. Here if, trustier value is smaller than threshold trustier attribute then, that means sender is trustworthy in communicating network. After declaring that vehicle is trustworthy, message will be sent to CA for updating both fields (counter field and trustier attribute field) via RSU. After updating message will be forwarded back to the monitoring center and then monitoring center will send this updated certificate to the receiver and sender via RSU. Here counter value defines that how many time one anonymity key is using by sender for transmitting the information in communication network.

But if trustier value is not smaller than threshold trustier value then, that means sender is not trustworthy and network is not safe. After this unfair result warning message will be sent to CA through monitoring center. Then CA will revoke all the certificate of that vehicle as describes in subsection III-A.

If message is not semantic and not authenticate then, warning notification will be sent to certificate authority via RSU. After that, CA will revoke all the certificate of the sender as describes in subsection III-A.

But after increasing the counter value, if sender finds that counter value is not smaller than threshold counter value then, pseudonym value with associated certificate will be changed from sender and message will be sent again by using same above procedure with new pseudonym key.

A. How does CA revoke the vehicle?

According to [1] certificate revocation overhead will be considerably reduced by CA. For this work, a secret key S_m which represents the shared ID is generated by the CA for each vehicle m. Then hash function will be applied on S_m to produce the field Y that will add all the certificates of same vehicle. After this work, when CA finds warning notification of vehicle m then, it will revoke all certificates from the CRL having certificate related to share key S_m of revoked vehicle m. At last CRL list will be updated by CA and this list will be sent to all neighboring vehicles. This proposed solution reduces the size of CRL only for the entirely revoked vehicles portion.

IV. ALGORITHM

Paper 1 describes that before sending the information, CA will distribute the pseudonyms set (anonymity keys) to each vehicle and also will add the trustiest attribute field and counter field in vehicle s certificate. And CA also will keep initial counter value to 0 (zero) in counter field for all vehicles. After that, reputation module will check the authentication of message to confirm that message M_m has come from sender vehicle V_m and will also check that message is semantic or not. Semantic verification is done for confirming that message M has not been changed in its transit time or not. If message is semantic and sender is authenticating, then trustier value will be calculated by reputation system. In this, if trustier value is smaller than threshold trustier value then, positive result will be generated. Such that on basis of this positive result we can ensure that vehicle is trustworthy. But if trustier value is not smaller then, negative output is generated. From this we ensure that vehicle is non-trustworthy. Here $p_{mt}2p_m$ is the pseudonym of vehicle m and k_i is key from which hash function (Hp_{mt}) will be calculated.

V. FLOW CHART

Before following steps of flowchart 6, message will be encrypted and also will be signed with private key of sender. Afer this sender will increase the counter value and also check that counter value is smaller than threshold counter value or not.

1) Step 1: Sender! Monitoring Center Encrypted message will be sent to monitoring center to check the authenticity of the sender.

2) Step 2: Monitoring Center! Reputation Module monitoring center contains reputation system. Transmit-ted message will be forwarded to reputation module. Here this module will check the authenticity and seman-tic property of message. After that, module will check trustier value of the sender.

3) Step 3: Reputation Module! Certificate Authority If sender is not trustworthy then, Message will be forwarded to CA for modifying the counter field and trustier attribute field.

If message is not trustworthy then, Warning message will be sent to CA for revoking that non-trustworthy vehicle.

Algorithm 1 Security in VANET

```
Step 1: INPUT: pmt will be hashed.
    H[Mm] = Hpmt (pmt jki)
    Hashed message will be encrypted by RSA algorithm.
    Enc[Mm] = F(H[Mm],e)= H[Mm]e mod n
    where, e is a prime number that is chosen in the range [3; (n)],
    (n) = (P-1) (Q-1),
    and n = P * Q
    Encrypted message will be signed by sender s private key.
    Dig[Mm] = Sigprikeym [Enc[Mm] OUTPUT : Trustworthy Vehicle
Step 2: Counter value cm will be increased by one and checked by sender before sending message.
    cm = cm + 1
    if (cm < C) then
    Sender sends encrypted data directly to monitoring center.
    Otherwise:
    Go to Step 7.
Step 3: Reputation module will check authenticity of sender.
    if (Recv[MAC[Dig[Mm]]]==MAC[Recv[Dig[Mm]]])
    then
    Reputation module will check the semantic property of message.
    otherwise:
        Jump to Step 6.
Step 4: if (VM(Dig[Mm])==[0,1]) then
    Reputation module will check the trustier value of sender.
    Otherwise:
    Go to Step 6.
Step 5: tv[m]=
    N
    X
    V M[Mmi] n N
    Mmi=M[m]
    if (tv[m] <= TV[m]) then
    Sender is trustworthy and Mm will be sent to CA for updating CF and TF.
    Updated Message will be sent to the receiver and sender.
    Otherwise:
    Go to Step 6.
Step 6: Warning notification will be sent to CA.
        CA will revoke all the certificate of the sender.
Step 7: pmt with certificate will be changed for vehicle m.
        Jump to Step 2
Step 8 END.
```

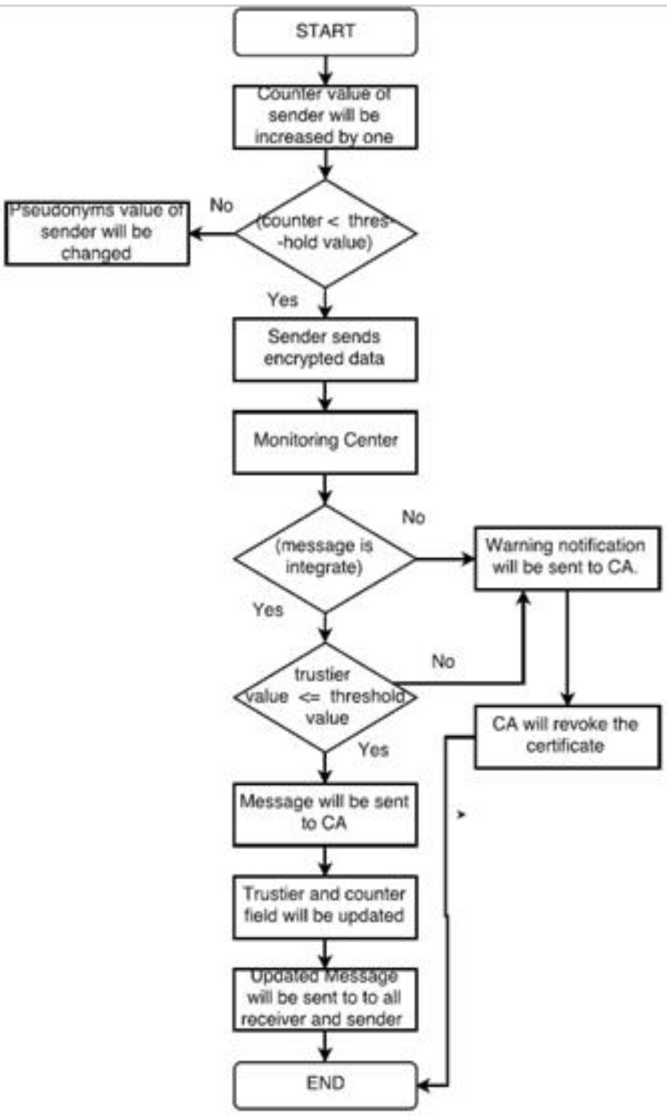
START
Counter value of sender will be increased by one
No
Pseudonyms value of sender will be changed
(counter < thres-hold value)
Yes
Sender sends encrypted data
Monitoring Center
No
(message is integrate)
Warning notification will be sent to CA
Yes
No
trustier value <= threshold value
Yes
CA will revoke the certificate
Message will be sent to CA
Trustier and counter field will be updated
Updated Message will be sent to to all receiver and sender
END

Fig. 6. Proposed Algorithm

VI. CONCLUSION AND FUTURE WORK

In this thesis, we have provided the more security on encrypted transmitted message by using reputation system with counter value. Here counter field has been used to indicate that how many times one anonymity key of a sender is used.

This all work has been done for finding the trustworthy vehicle in the VANET.

In the future work of this proposed work, we can include the time field in certificate such that message of trustworthy vehicle can be transmitted within threshold time. And we can also reduce the revocation overhead as we are seeing in this proposed work where is a part of message is not semantic then, whole vehicle is being revoked. Here we can add some idea such that only non-trustier message can be revoked.

ACKNOWLEDGMENT

Predominantly, my sincere thanks and regards to my Faculty Members for their guidance and support during my thesis session.

Secondly, I would like to express my sincere appreciation and thanks to my friends for his/her help and support.

Finally, I'm grateful to my family members for insisting me to work hard in my thesis. It was impossible for me to complete this thesis work without their love, blessings and encouragement. And thanks to God, for always showing up his presence by infusing me with power.

REFERENCES

[1] Abdulhussain, Sadiq H."Enhanced Management of Certificate Caching and Revocation Lists in VANET." International Journal of Computer Applications83.12 (2013).

[2] Assila, Ahlem, Ihssen Jabri, and Arafet Ltifi. "Secure architecture dedicated for VANET alarm messages authentication through semantic verification. "Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on. IEEE, 2012.

[3] Wang, Z., Liu, L., Zhou, M., Ansari, N. (2008). A position-based clustering technique for ad hoc intervehicle communication. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 38(2), 201-208.

[4] Barnwal, Rajesh P., and Soumya K. Ghosh. "Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks." Connected Vehicles and Expo (ICCVE), 2012 International Conference on. IEEE, 2012

[5] Ruj, S., Cavenaghi, M. A., Huang, Z., Nayak, A., Stojmenovic, I. (2011, September). On data-centric misbehavior detection in VANETs. In Vehicular technology conference (VTC Fall), 2011 IEEE (pp. 1-5). IEEE.

[6] Lin, Xiaodong, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. "Security in vehicular ad hoc networks." Communications Magazine, IEEE 46, no. 4 (2008): 88-95.

[7] Jaballah, Wafa Ben, Mauro Conti, Mohamed Mosbah, and Claudio E. Palazzi. "A secure alert messaging system for safe driving." Computer Communications 46 (2014): 29-42.

[8] Yan, Tan, Wensheng Zhang, and Guiling Wang. "DOVE: Data dissemination to a desired number of receivers in

vanet.” IEEE Transactions on Vehicular Technology, 63.4 (2014): 1903-1916

[9] Daeinabi, Ameneh, and Akbar Ghaffarpour Rahbar. ”An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks.”Computers and Electrical Engineering 40.2 (2014): 517-529

[10] Daeinabi, Ameneh, Akbar Ghaffar Pour Rahbar, and Ahmad Khademzadeh. ”VWCA: An efficient clustering algorithm in vehicular ad hoc networks.” Journal of Network and Computer Applications 34.1 (2011): 207-222.

[11] Rawashdeh, Zaydoun Y., and Syed Masud Mahmud. ”A novel algorithm to form stable clusters in vehicular ad hoc networks on highways.” EURASIP Journal on Wireless Communications and Networking 2012.1 (2012): 1-13.

[12] Bali, Rasmeet S., Neeraj Kumar, and Joel JPC Rodrigues. ”Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions.” Vehicular communications 1.3 (2014): 134-152.

[13] Huang, Zhen, Sushmita Ruj, Marcos A. Cavenaghi, Milos Stojmenovic, and Amiya Nayak. ”A social network approach to trust management in VANETs.” Peer-to-Peer Networking and Applications 7, no. 3 (2014): 229-242.

[14] Dotzer F, Fischer L, Magiera P (2005) Vars: a vehicle ad-hoc network reputation system. In: IEEE international symposium on a world of wireless mobile and multimedia networks, pp 454456.

[15] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. ”Sur-vey on VANET security challenges and possible cryptographic solutions.” Vehicular Communications 1.2 (2014): 53-66.

[16] Schmidt, Robert K., et al. ”Vehicle behavior analysis to enhance security in vanets.” Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008). 2008.

[17] Ghosh, Mainak, Anitha Varghese, Arobinda Gupta, Arzad A. Kherani, and Skanda N. Muthaiah. ”Detecting misbehaviors in VANET with integrated root-cause analysis.” Ad Hoc Networks 8, no. 7 (2010): 778-790.

[18] Daeinabi, Ameneh, and Akbar Ghaffarpour Rahbar. ”Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks.” Multimedia tools and applications 66.2 (2013): 325-338.

[19] Laberteaux, Kenneth P., Jason J. Haas, and Yih-Chun Hu. ”Security certificate revocation list distribution for VANET.” Proceedings of the fifth ACM international workshop on Vehicular Inter-Networking. ACM, 2008.

[20] Al-Khassawneh, Yazan Alaya, and Naomie Salim. ”On the use of data mining techniques in vehicular ad hoc network.” Advanced Machine Learning Technologies and Applications. Springer Berlin Heidelberg, 2012. 449-462.

[21] 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.

[22] Louazani, Ahmed, Sidi Mohammed Senouci, and Mohammed Abder-rahmane Bendaoud. ”Clustering-based algorithm for connectivity maintenance in vehicular ad-hoc networks.” Innovations for Community Services (I4CS), 2014 14th International Conference on. IEEE, 2014.