A Cluster Based Group Signature Mechanism For Secure Vanet Communication

Navjot Kaur, Sandeep Kad

Abstract: Vehicular adhoc network is one of the recent area of research to administer safety to human lives, controlling of messages and in disposal of messages to users and passengers. VANETs allows communication of moving vehicular nodes. Movement of nodes leads in changing network size and scenario. Whenever a new node joins the network, there is a threat of malicious node attack. So, we need an environment that is secure and trust worthy. Therefore a new cluster based secure technique is proposed where cluster head is responsible for providing communication between the vehicular nodes. Performance parameters used in this paper are message drop ratio, packet delay ratio and verification time.

Keywords: Cluster, Cluster Head, Trusty authority, Vehicular nodes

I. INTRODUCTION

In adhoc domain, information shared is conscious. Sharing of information makes security as one of the major concern for vehicles, as each vehicle is the representative of network. In Vehicular network nodes have dynamic mobility. The moving Vehicular node transmit and receive data. Whenever nodes join or leave the network, network size enlarges and reduces automatically. The change in the network size causes the change in the nature of nodes. Therefore if the bad-natured vehicular node joins the network, it can send bogus messages, giving harm to the network [2, 4]. Accordingly there is need to secure the privacy of information to be transmitted [5]. In the given paper, a new cluster based group signature technique has been proposed. Group signature is an encouraging technique to enable nameless authentication. It allows either group member to sign the message on behalf of the whole group without exposing the identity of the group. As the network size increases, it becomes more challenging to secure the information. Therefore the proposed technique is deployed [9, 13]. Figure1 shows scenario of cluster based group signature. Mobile nodes that are adjacent to each other in geological regions design groups, hence forming cluster based group signature. Moreover it has been proved that cluster based group signature increases the performance of the overall network [1].

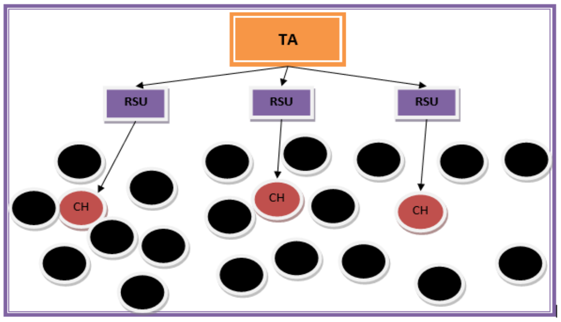

Figure1: *Cluster based group signature*

- *Navjot kaur, M.Tech Scholar, Amritsar College of Engineering and Technology, India. PH-8557920405. E-mail: kaur.navjot30590@gmail.com*
- *Sandeep Kad, Asoociate professor, Amritsar College of Engineering and technology, India.*

The scenario of VANETs in this paper consist of:-

TA-trusted Authority
CH-Cluster Head
RSU-Road Side Unit
OBU- On Board units

- **TA** (Trusty Authority) is the management centre. It generates certification and keys and forward it to the Cluster Head for OBUs when they join the network. It divides the whole precinct into several cluster. Cluster Head (CH) is selected by TA on the basis of reputation value. TA is authoritative in terms of communication, computation and storage [13]**.**
- **CH** is selected in by TA. CH uses the certification to generate unique signature or key for each node in the cluster, that will be matched when any transmission will take place. CH passes any data packet to the node that has unique key which cluster head provides when they register on the network.
- **RSUs** (Road Side units) administer vehicles within their communication area. They are the bridges between TA and CHs. RSUs are responsible to issue certificate and keys for OBUs when they join the network [13].
- **OBUs** (On Board Units) repeatedly broadcast traffic safety related information to the users and the passengers, thereby improving the road side communication [13].

For communicating with the other cluster, CH pass the information to RSU and Communicate with other RSU which further communicate with CH and pass the information only to the authenticated node. In this paper section II shows the related work. Section III highlights the existing technique used. Section IV focused on problem formulation. Section V contains proposed technique. At last section VI test bed results based up on proposed technique and existing technique and section VII compresses the conclusion and future scope of VANETs.

II.RELATED WORK

P.Vinod et al. [7] used priority batch verification algorithm to protect the system from malicious vehicles that send false messages to the other vehicles. Batch verification and key agreement scheme authenticate several request sent from different vehicles. Atsuko et al. [9] proposed an application friendly GS. It has provided solutions for real life problems. GS aggregated linking, direct opening, revocking and batch verification. The link manager calculates the genuine node and attacker node. Neeraj et al. [11] proposed an algorithm to overcome the new attacks via low latency passing and reducing bandwidth of authentication. As in VANETs some serious attacks can occur. Asif et al [12] proposed a framework that utilizes both traditional and cryptographic schemes, asymmetric PKI and symmetric respectively. The asymmetric cryptography scheme is used for security exchange and symmetric for low latency safety applications. Yeongkwun et al. [5] discussed the fail-safe security issue. Security in VANETs raises the importance of privacy. As the information transmitted is sensitive and can affect the security decisions. Mario et al. [4] proposed technologies and protocols for content distribution. Other aspects covered in the paper include coexistence of Wi-Fi and LTE, network coding and pollution attacks. Xiaoyan et al [13] proposed a scheme to divide the whole domain into RSUs for distributing the key and to manage the vehicles. It has used hash message authentication to avoid time consuming CRL. Also adopted Co-operative message authentication. Rong et al. [1] discussed a cluster based scheme for data transmission. He has presented a cluster head selection algorithm and switching algorithm. CH selection algorithm elects node degree, candidate CHs and difference among them. It has also focused on Qos requirements. Brijesh et al. [2] discussed group signature for privacy preservation. Group signature provides security, uniqueness to broadcast information. It verifies the effectiveness and overheads. Thus increasing the efficiency. Kakkageri et al. [6] has stressed on safety applications such as reliability, security, trust, real time delivery and latency. The research efforts are made on information management techniques including gathering, aggregation, validation and distribution.

III.EXISTING WORK

Group signature increases the level of security of a network. In this the domain of network is divided into groups and any group member can sign the message on behalf of the whole group. It allows the identity of the group member to be hidden. Here the information can be revealed or identified only by the genuine node [2,4,9,13]. Now if the attacking node tries to attack the privacy of information then it will first be verified. Group signature allows only the authenticated and genuine node to access the information that is to be transmitted between the vehicular nodes. It provides security to broadcast a message in a network between the source and destination [2,4,9,13] Figure 2 shows that the network is divided into number of nodes having some protocol system. The nodes are secured through group signature. For any transmission to take place an authentication check is made on the nodes. If the nodes are found authenticated transmission is allowed otherwise not.

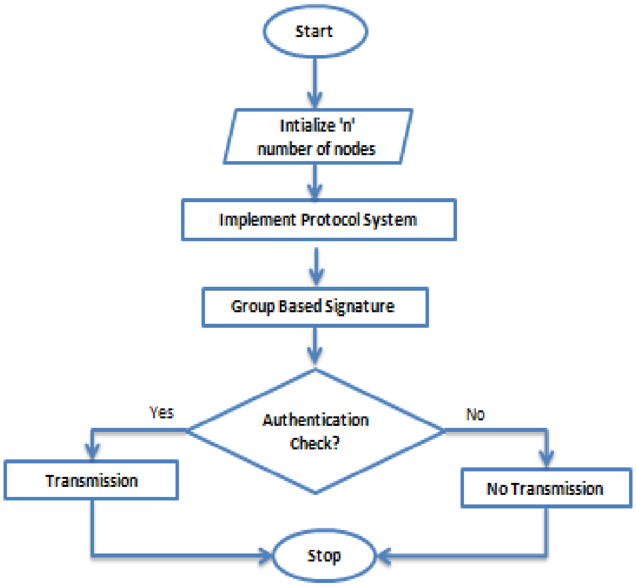

Figure 2: *Group Signature Flow Diagram [10]*

IV PROBLEM FORMULATION

VANETs is an open medium allowing communication between the vehicles. Due to open access, there is threat to the privacy of message and identity of node, if the network is not perfectly protected. Thus need for secure technique arises.[3, 5]. Group signature is an effective technique for securing a system. It allows any group member to sign the message on behalf of the whole group without disclosing the identity of the group [4, 13]. The problem arises when the network size increases. With the change in network size, network scenario also changes. Here the possibility of malicious node attack occurs. Now in order to provide better security to the system the concept of clustering is used with group signature.

V. PROPOSED WORK

As discussed in the existing system, the level of security depends upon the trust factor between the nodes, and this trust factor is not so easy to measure. So there is a need to build a high level improved secure technique in order to generate a secure environment between the nodes. For this, a new cluster based technique is proposed to enhance the level of security. This proposed technique will overcome the shortcoming of the previous technique of group signature.

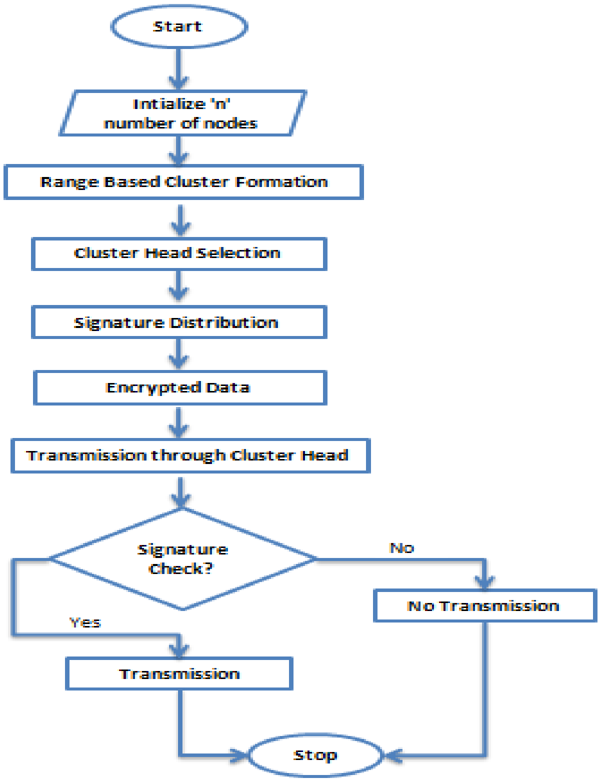

Figure 3: *Cluster Based Group Signature Flow Diagram*

As shown in figure 3, the network is divided into range of clusters thus enabling security on each cluster. The cluster head is selected on the basis of the reputation value (i.e., calculated on the basis of nodes previous transmissions) by the trusty party. And all the transmission in a cluster will be done by the cluster head. The cluster head passes any packet to the vehicular node only if the node has the key which the cluster head provided it when they registered on the network. The registration and certification of the node is done by the trusty party. Also the trusty party signate the cluster head. Now suppose, if the communication is to take place with the other cluster, then the cluster passes the information to RSU and communicate with other RSUs which further communicate with the CH and pass the information to the authenticated node. This technique does not allows direct transmission between the nodes. If there is direct transmission, then there is a threat to the information to be communicated and to the valid/genuine node [8,10]. The Proposed technique of new cluster based group signature will enhance the overall performance of the network in terms of following parameters:

- Message drop ratio
- Packet delivery ratio
- Verification time

VI. SIMULATION AND RESULTS

The parameter and values utilized for a cluster based group signature is shown in table1.

Table1: *Simulation Parameters and values*

Parameter	Value
Channel	Wireless
Propogation Model	Radio Propogation Model
Network Interface	Wireless Physically
MAC	802.11
Queue	Priority
Link Layer	LL
Antenna	Omni Antenna
Queue Length	500
No of Nodes (nn)	50
Protocol	DSR
Area	2000*1500

In the given figure, TA elects the Cluster Head for every cluster. The count of cluster heads rely upon the count of clusters. The CHs are elected form the prior reputation value. In the given figure the domain is divided into three clusters having their individual cluster heads [8, 10].

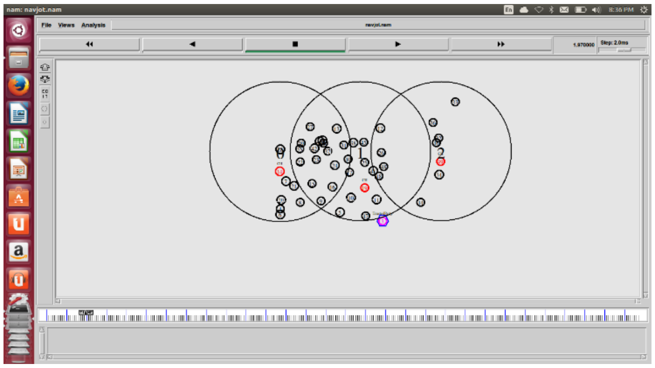

Figure 4: *Range Based Clusters*

After electing CHs, TA generate signature for each cluster head. Receiving after, cluster heads distribute these keys to their group of nodes. On acquiring the key, each node defer it to the trusty party. These keys are cured in the database of trusty party and during communication, the keys are checked by the trusty party [8, 10]. Now to present communication between the source and destination. The source node first sends the request to its neighboring nodes. The neighboring nodes to their neighbors, for reaching to destination. Once the request approaches the destination it cause it to go along its keys. This results in providing most secure and optimized route for communication [8, 10].Finally when the route is tracked, data transmission starts. Data can be of any type audio, video, infotainment etc. The Simulaton is performed using NS 2.35. The simulation results are in terms of Message Drop Ratio, Packet Delay ratio and Verification time.

Message Drop Ratio

It is the number of packets that are sending but not received at the destination [10].

$$\text{MDR} = \sum \text{Number of packet not received} \\ / \sum \text{Number of packet send}$$

Delay Ratio (%age)

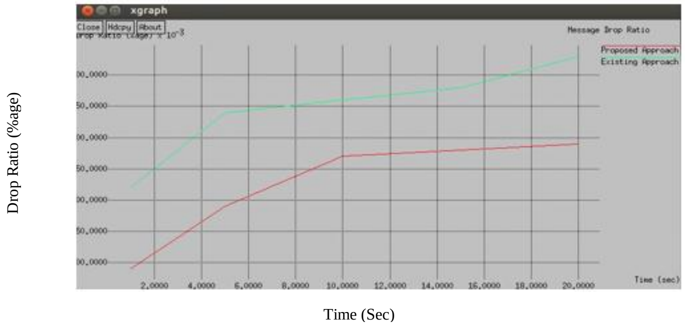

Figure 9: *Message Drop ratio*

Existing approach have more message drop ratio as compare to proposed approach as shown in the above figure [2, 8, 10].

Table 2: *Comparasion on the basis of Message Drop ratio*

Time(Sec)	Message Drop Ratioof Group Signature(%age)	Message Drop Ratio of Cluster Based Group Signature(%age)
1	22	09
5	34	19
10	36	34
15	39	37
20	45	41

Packet Delay Ratio

The average time taken by a data packet to arrive in the destination. It cover the delay caused by route discovery process and the queue in data packet transmission. The data packets that are successfully delivered to destinations are considered [8, 10, 13].

$$PDR = \sum(\text{arrive time} - \text{send time}) \,/ \sum \text{Number of connections}$$

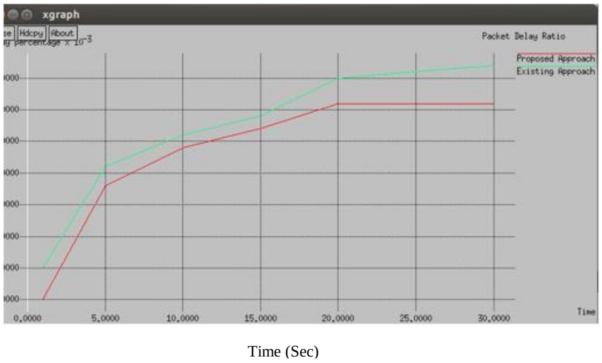

Figure 10: *Packet Delay Ratio*

Existing approach have more packet delay ratio as compare to proposed approach as shown in the above graph. As the proposed technique shows less delay time. Therefore it increases the performance of the network.

Table 3: *Comparasion on the basis of Packet Delay ratio*

Time(Sec)	Delay Ratio of Group Signature(%age)	Delay Ratio of Cluster based Group Signature(%age)
1	15	1
5	31	28
10	36	34
15	39	37
20	45	41

Verification Time

It is explained as the total amount of time taken by clusters to verify their keys by TA [10, 13].

VT is calculated as: $\text{Total (VT)} = T_{C1} + T_{C2} + T_{C3}$

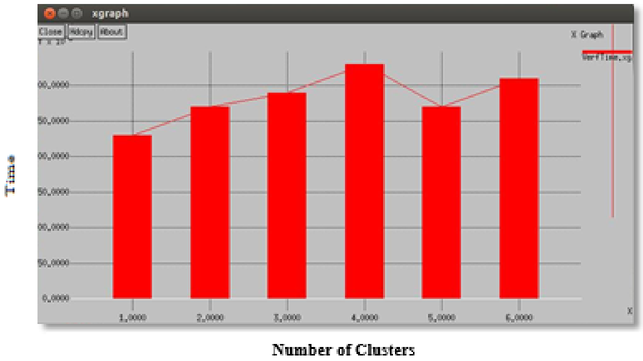

Figure10: *Verification Time of existing technique and proposed technique*

The above figure shows that the existing approach has higher verification time for each cluster as compare to proposed approach.

Table 4: *Comparasion on the basis of verification Time*

Number of Cluster	Verification Time taken by Group Signature(Sec)	Verification Time(taken by Cluster based Group Signature Sec)
1	27	23
2	33	29
3	31	27

VII.CONCLUSION

In this paper, a comparative study is shown between group signature and cluster based group signature. Group signature provides secure environment for VANETs by signing the message on behalf of the whole group. But it becomes more challenging to secure the network when the network size increases. So, cluster based secure environment is proposed where each cluster head is responsible for providing the communication between the nodes. The performance results are shown by message drop ratio, packet delay ratio and verification time. And it is observed that the proposed cluster based group signature mechanism shows significant improvement as compared to group signature.

REFERENCES

[1] Chai R., Yang B., Li L., Sun X., Chen Q., “Clustering-based Data Transmission Algorithms for VANET" IEEE, 2013.

[2] Chaurasia B., "Message broadcast in VANETs using Group Signature" IEEE, pp. 131-135, 2008.

[3] Feiri .M., Schmidt . R., Kargl . F., “ The Impact of security on Cooperative Awareness in VANET” IEEE vehicular Adhoc Conference, 2013.

[4] Gerla M., Wu C., Pau G., “Content Distribution in VANETs" pp. 3-12, 2014.

[5] Kim Y., Kim I., “Security Issues in Vehicular Networks" IEEE, pp. 468-472, 2013.

[6] Kakkasagerim M., Manvi S., “ Information management in vehicular adhoc network: A review” Journal of Network and Computer Application ” 2013.

[7] Kumar P., Maheshwari M., “Prevention of Sybil Attack and Priority Batch Verification in VANETs”, IEEE, 2014

[8] Kaur N., Kad S., “A review on security related aspects in vehicular adhoc network”, 1st International Conference on Information Security & Privacy 2015, Vol. 78, pp. (387–394) 2016..

[9] Mamun S., “ Secure VANET Applications with a refined Group Signature” Twelth Annual Conference on Privacy, Security and Trust, pp. 199-206, 2014.

[10] Kaur N., Kad S., “A new Cluster based secure technique in vehicular adhoc network, IEEE proceedings of Sixth International Conference on Communication Systems and Network Technologies (CSNT’16), 2016 [Accepted].

[11] Varshney N., Roy T., Chaudary N., “Security Protocol for VANET by Using Digital Certification to Provide Security with Low Bandwidth”, International conference on communication and sigbal processing”, pp. 768-772, 2014.

[12] Wagan A., Jung L., “Security Framework for Low Latency VANET Applications” IEEE, 2014

[13] Zhu X., Jiang S., Wang L., Li H., Zhang W., Li Z., " Privacy-Preserving Authentication Based on Group Signature for VANETs" IEEE Wireless Networking Symposium, pp. 4609-4614, 2013