Euler's Totient based Group Formation Scheme in VANET

Thounaojam Korouhanbi Devi
M.Tech Student
Lovely Professional University

Shabnam Sharma
Assistant Professor and Research Scholar
Lovely Professional University

Aditya Prakash
Lecturer
Lovely Professional University

ABSTRACT

Vehicular ad-hoc network is an emerging technology that facilitates vehicles within the network range to communicate with one another or with the roadside infrastructure, sharing useful information. It is indispensable to ensure reliable and secure implementation of VANET. Authentication is one of the salient aspects of security, which ensures that the communicating entities are the ones that they claim to be. This paper proposes a scheme for cluster formation in VANET, to perform group authentication. A group based authentication provides anonymity and conditional privacy to the vehicles. The cluster heads are computed by determining the generators of the group using cyclic group concept under additive property. Group generators are the ones that can generate all the elements in the group. Once, the cluster heads are selected, vehicles forming part of the cluster will be determined based on Euler's totient function.

General Terms

Cluster formation using cyclic group function with respect to additive property

Keywords

Cyclic group, Euler's totient function, RSU, VANET

1. INTRODUCTION

The developments in the fields of wireless communication technology and automobile industries, led to the use of wireless devices in vehicles. This allows vehicles under specified range to form a vehicular network, where vehicles can communicate with the roadside infrastructure as well with other vehicles that are part of the network. Such a network is termed as Vehicular Ad-hoc Network, acronym as VANET. VANET is a rapidly growing technology with a number of applications. It has emerged as an active field of research because of its application in improving traffic efficiency, road safety and other services like location based services, navigation etc. Some of the research areas in VANET are focussed on architecture, routing, broadcasting, Quality of Service (QoS), and security issues.

In VANET, every vehicles that comes under the range of approximately 100-500 metres acts as a wireless router or node, which facilitates them to connect and create a large vehicular network. Each vehicle that are part of the network serves as either a sender, a receiver or a router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. Vehicle that falls out of the signal range are dropped out of the network. Any vehicle that comes under the network range can join in.

1.1 Components of VANET

1.1.1 On Board Unit (OBU)

Devices mounted on vehicles to facilitate communication with other vehicles and RSUs.

1.1.2 Road Side Unit (RSU)

Communication units located aside the road that connects with the application server and trust authority.

1.1.3 Trusted Authority (TA)

TA performs certificate generation, distribution and revocation.

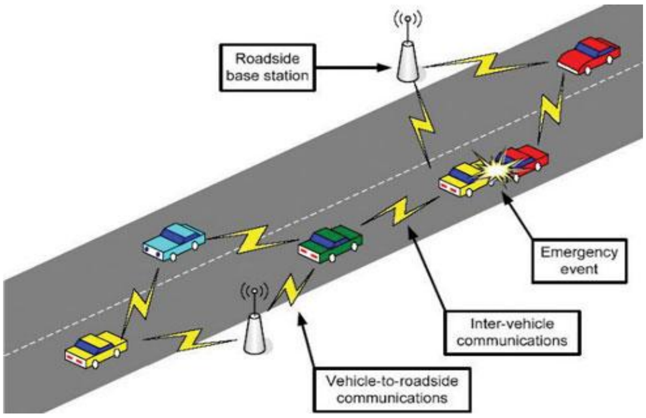
Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Fig. 1 A diagrammatical representation of VANET architecture

1.2 Types of communication

Communication in VANET can be configured in three ways. These include:

- Inter-Vehicular communication: Vehicle-to-Vehicle communication (V2V)
- Vehicle-to-Roadside communication: Vehicle-to-Infrastructure communication (V2I)
- Routing-based communication

VANET provides numerous safety-related and non-safety related applications [12]. Safety-related applications involves avoiding road accidents, which is a life threatening situations. Non safety-related applications includes information about an expected traffic jam, location based services etc. In order to implement VANET in such a way so as to fully utilize it, we need to focus on the security aspects of VANET. The vital information that is being shared by the vehicles should not be modified or altered by any malicious user. A malicious user can be any attacker who tries to gain unauthorised access and misuse the network. There are three main types of attackers in VANET viz. insider versus outsider, malicious versus rational, active versus passive. Attacks in VANET can be classified into three categories viz. threats to availability, confidentiality and authenticity.

The remainder of this paper is organized as follows: Section 2 presents previous works on authentication schemes for VANET. In Section 3 we discuss the proposed algorithm. Section 4 discusses the results and performance. Section 5 and 6 presents conclusion and discusses about the future work that can be carried out.

2. RELATED WORK

Many research works has been carried out till date to provide authentication in VANET.

The Public key infrastructure is used to ensure user validity. It is based on the concept of asymmetric key cryptography and Digital signature Algorithm. Certificate Revocation Lists (CRLs) are used to revoke registration of misbehaving vehicles. RSUs maintain CRLs. But the problem with PKI is that it requires large memory storage area for key and certificate storage [9].

Efficient & Robust Pseudonym authentication in VANET is concerned with efficient and easy-to-manage security and privacy-enhancing mechanisms as they are essential for the widespread adoption of VANET. It uses pseudonym authentication and group signature. Efficient Conditional Privacy Preservation Protocol uses bilinear pairing and group signature as the cryptographic basis for providing fast anonymous authentication& privacy tracking, to minimize required storage for short time anonymous keys [3].

ECPP issues on the fly short time anonymous certificates to OBUs by using a group signature scheme. Since RSUs can check the validity of the requesting vehicle during the short time anonymous certificate generation phase, such revocation check by an OBU itself is not required. ECPP doesn't provide unlinkability & traceability [11].

VANET authentication using signature and TESLA++ (VAST) [1] is an improvement to time efficient stream loss tolerant authentication (TESLA). It uses elliptic curve digital signature algorithm (ECDSA) to provide fast authentication and non-repudiation. TESLA uses symmetric key cryptography with delayed key disclosure to provide necessary asymmetry. But it is not resilient to DoS attack as the receiver has to store the message till the key is disclosed. So TESLA++ was introduced to mitigate DoS attack by just storing self generated MAC of the message. But again TESLA++ cannot provide non-repudiation so ECDSA was used.

A novel RSU-based message authentication scheme for VANET was proposed to enable the message authentication in intra and inter RSU range, and the handoff within the different RSUs. It makes the balance in the overhead of computation and communication and the security against the attacking. It uses Diffie-Hellman key establishment protocol [4] for secure exchange of keys and HMAC. HMAC is a fast and effective message authentication scheme. Secure Privacy and Distributed Group Authentication for VANET aims at providing group authentication, message integrity and conditional privacy [5].

Hui Zhu proposed the Privacy preserving authentication scheme (PPAS) that performs local authentication and roaming authentication based on bilinear pairing. It makes use of bilinear pairing and ECDSA. It provides an effective protection of privacy and anonymity among vehicles and infrastructure. Anonymous authentication is one of the significant methods to preserve privacy, which is a key problem of large scale application of VANET [6].

Lai proposed a new scheme that performs batch verification based on bilinear pairing and batch authentication. This algorithm improves the quality of traffic. It also verifies message in group, thus limiting the chances of information delay. This scheme provides message authentication, privacy preservation, auditability and prevents replay attack. In future we can work on to identify illegal signature and designing more efficient scheme [8].

Group authentication algorithm (GAP) is a distributed authentication scheme. It uses session based pseudonym to support anonymous communication. Batch verification method is used which helps in significantly reducing the message delay. It enables the vehicle to verify a large number of messages in the case of high vehicular density and also improves message loss ratio. GAP can efficiently handle the growing CRLs while achieving conditional traceability by the trust authority. Instead of demanding a huge buffer space at each vehicle, this protocol can keep the required key storage a minimal without losing its privacy. In GAP all the vehicles that comes under the range of the same RSU forms a group. In this paper, a new cluster forming scheme is proposed using mathematical operation to group vehicles in a VANET system [7].

3. PROPOSED METHODOLOGY

The proposed algorithm aims to provide an efficient scheme for authentication and privacy preservation in VANET based on group authentication scheme.

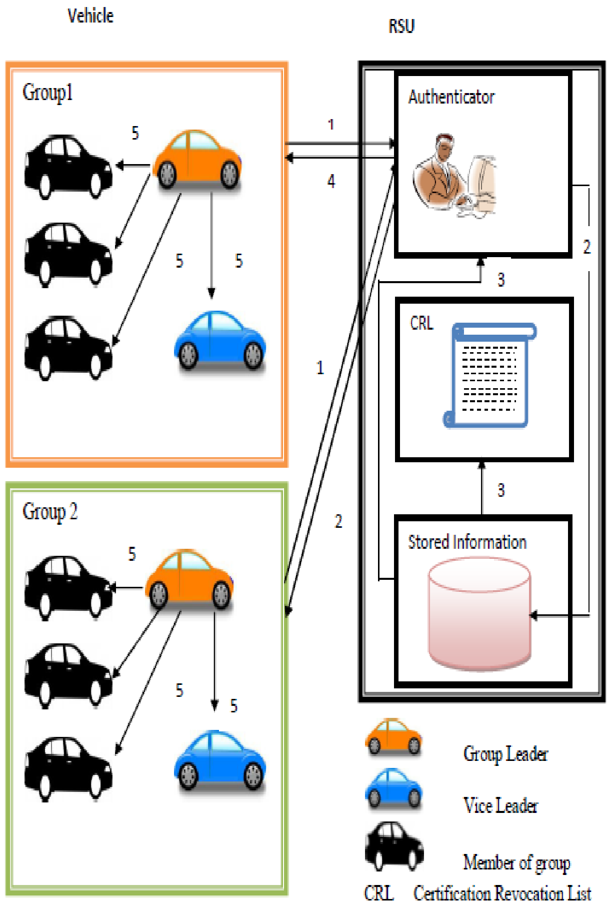

Fig. 2 Architecture of Proposed algorithm

1. Vehicles forwards encrypted message to RSU.
2. RSU decrypts it, authenticator compares with the stored information.
3. If it is valid, then request is accepted else rejected and CRL is updated.
4. Information forwarded to vehicles.
5. Vehicles forms group, group leader and vice leader are assigned.

3.1 System Architecture

The main components of the proposed scheme comprises of vehicles, RSU and authenticator. When a vehicle comes under the range of an RSU, it first registers itself with that RSU. The vehicle sends its unique number to the RSU. Further the RSU forwards it to the authenticator. The unique number is then compared with the information stored in the database. If the unique number matches, then it is authenticated otherwise the request is revoked.

3.2 Proposed Algorithm

3.2.1 Vehicle Authentication

The user creates a message, M consisting of timestamp T_s, vehicle's number N and a randomly generated prime number P of the form $M=\{T_s,N,P\}$. This message is then encrypted using Public key, PU_{RSU}. The encrypted message is then forwarded to the RSU where it is decrypted using Private Key, PR_{RSU}.

```
Begin
  Vehicle input $M = \{T_s,N,P\}$
    Perform encryption $e = E(M,PU_{RSU})$
    Forward e to RSU
  RSU perform decryption $d=D(e,PR_{RSU})$
    Compare N with stored information in database
    If N is valid then
      Calculate $MI_{RSU}$, generate UID
        Forward UID, $MI_{RSU}$ to user
        User computes $MI_U$
          If $MI_{RSU} = MI_U$ then
            Keep UID, determine maximum member of
            group
            Compute group generator, assign group
            leader, Vice leader
            Generate member of group
            Perform signing and verification
           End if
           Else
            Reject the request
  End if
  Else
    Reject the request, update CRL
End
```

Fig. 3 Proposed algorithm

The user is authenticated by comparing N with information stored in the database. Once the authenticity of the user is proved, RSU calculates the multiplicative inverse [18], MI_{RSU} generates unique identification number, UID for every new user registered. This information is forwarded to user. The user then computes multiplicative inverse of its P, MI_U and is then compared with MI_{RSU}. If the exact match is found, then, further operations are executed otherwise, the request is rejected.

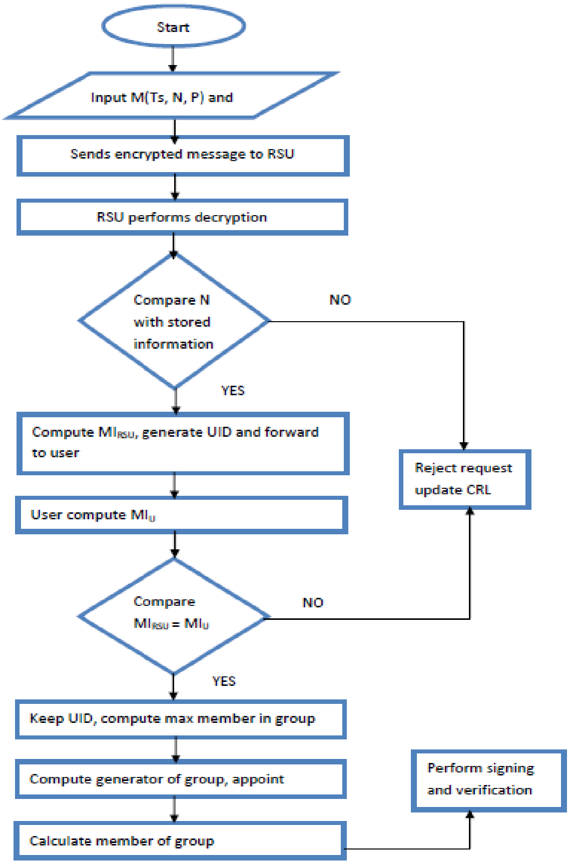
Start
Input M(Ts, N, P) and
Sends encrypted message to RSU
RSU performs decryption
Compare N with stored information
NO
YES
Compute MI_{RSU}, generate UID and forward to user
Reject request update CRL
User compute MI_U
Compare $MI_{RSU} = MI_U$
NO
YES
Keep UID, compute max member in group
Compute generator of group, appoint
Perform signing and verification
Calculate member of group

Fig. 4 Flowchart representing the Proposed Algorithm

3.2.2. Selection of Group Leader

From group, $G=\{Z_N,+\}$,where Z_N denotes the maximum number of vehicles that are the part of same group, selection of Group Leader and Vice Group leader is done on the basis of Cyclic Group Property with respect to additive operation [10]. Cyclic group is a group that is generated by a single element g, called the generator of the group [13]. All the elements of the group may be obtained by repeatedly applying the group operation or its inverse to g. More than one generator may exist in a group. In such case, one of the generator is selected as the group leader and the other is elected as vice leader.

3.2.3. Determine Group member

Vehicles belonging to the group are computed using Euler's totient function Φ(n) [2]. Euler's totient function Φ(n) is defined as the number of positive integers less than n and relatively prime to n. Once group leader is determined, members of the group are computed.

3.2.4. Message signing and Authentication

Messages sent by any vehicles belonging to a group will be signed with a common signature for that group.

4. RESULT AND DISCUSSION

This section discusses the results that are obtained during implementation of the proposed algorithm in MATLAB. The variation in the time taken for formation of cluster and selection of cluster with respect to different number of vehicles has been analysed.

Table1. Encryption and Decryption time recorded during simulation

Process	Time (Seconds)
Encryption	0.10178
Decryption	1.8713

Table 2: Time Taken for cluster Formation w.r.t no. of vehicles

No. of vehicles	Cluster Formation Time (Seconds)
3	2.8863
5	2.9445
6	2.975
7	3.1518
10	3.3945
12	3.8381

Table 3: Time taken for selection of cluster heads w.r.t no. of vehicles

No. of Vehicles	Cluster Head Selection Time (seconds)
3	0.27225
5	0.14193
6	0.20892
7	0.27107
10	0.3338
12	0.3982

Table 1, 2 and 3 illustrates the values of time in seconds recorded for different processes during implementation of the proposed algorithm. In table 1 the time taken during the process of encryption and decryption are recorded. Table 2 shows the time taken by varying number of vehicles to form cluster. Table 3 represents the time taken by each cluster to select a cluster head with respect to the number of vehicles in the cluster.

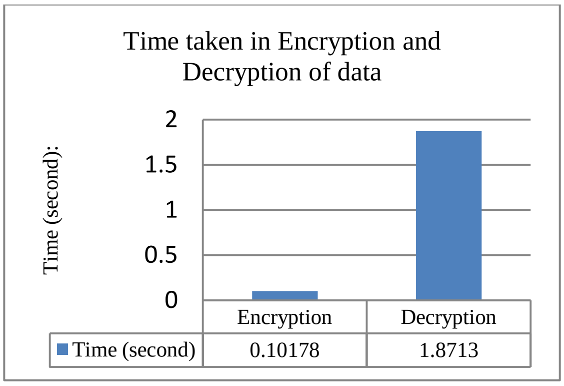

Fig. 5 Graph depicting the time taken in encryption and decryption of data

The above figure represents the analysis of time taken during the encryption and decryption process. RSA algorithm was used during simulation for encrypting the message, comprising of the timestamp, vehicle number and a prime number. This message was encrypted and forwarded to the RSU for further processing. RSU decrypts the message and compares the vehicle number with the numbers store in the database, and validates it.

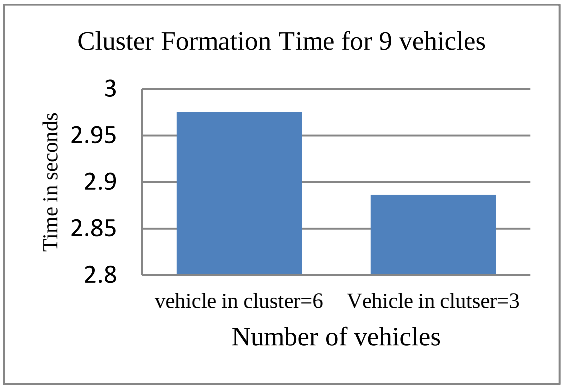

Fig. 6 Graph illustrating the time taken in Cluster formation for 9 vehicles

Figure 6 illustrates the time taken for the formation of cluster. A counter was kept by the RSU to count the number of vehicles that registers with it. The cluster is then form based on the coordinates i,e the location. When 9 vehicles are deployed in the network, 2 clusters were formed. The first cluster comprises of 6 vehicles and the second cluster comprises of 3 vehicles. After the clusters were formed, a cluster head was selected for each cluster. The cluster heads are selected based on the concept of cyclic group with respect to additive property, where a generator of the group is generated. The generator is the number that can generate all other members of the group. For the first cluster the algorithm takes 0.20892 seconds and for the second cluster the algorithm takes 0.27107 seconds for selection of cluster head.

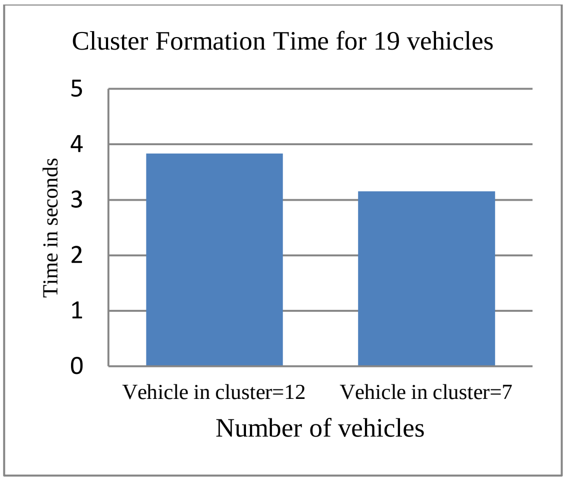

Fig. 7 Graph illustrating the time taken in Cluster formation for 19 vehicles

The above graph illustrates the time taken to form cluster, when 19 vehicles were deployed in the network. 0.3982 seconds and 0.3338 seconds are taken by each cluster to select a cluster head.

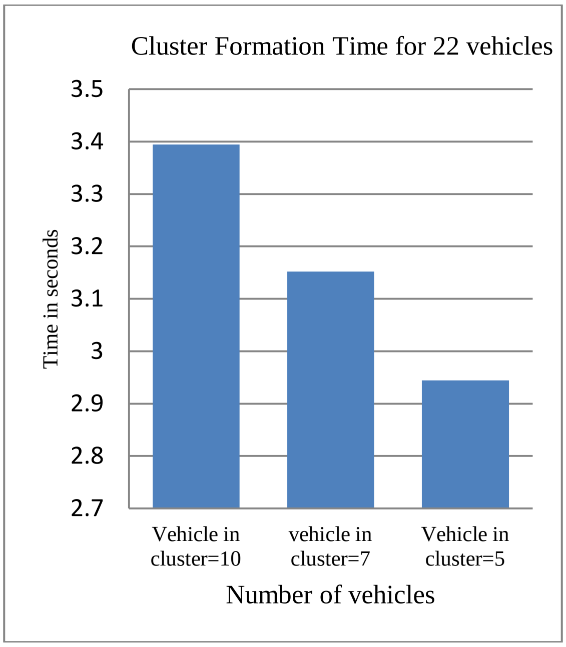

Fig. 8 Graph illustrating the time taken in Cluster formation for 22 vehicles

Figure 8 represents the time taken to form cluster when 22 vehicles are deployed in the network. 3 clusters are form comprising of 10, 7 and 5 vehicles respectively in each cluster. The 3 cluster takes 0.338, 0.27107 and 0.14193 seconds respectively for cluster head selection.

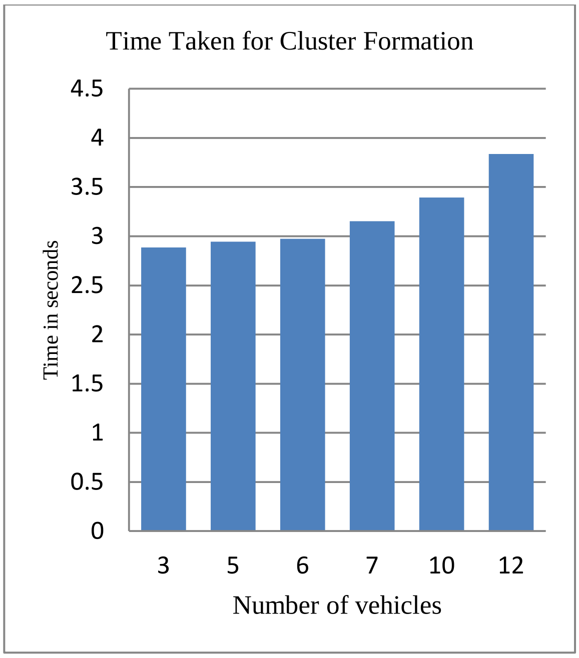

Fig. 9 Variation in time during Cluster Formation

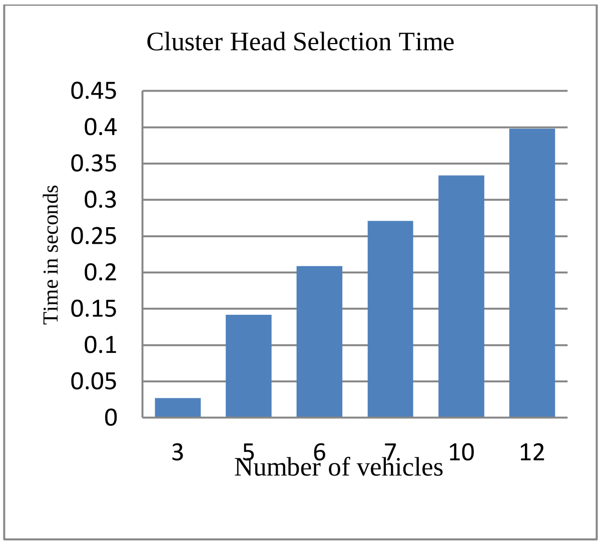

Fig. 10 Variation in time during selection of Cluster Head

Figure 9 and 10 illustrates the variation in time for cluster formation and selection of cluster head with respect to the varying number of vehicles.

5. CONCLUSION

To ensure a secure and reliable VANET, vehicles and messages needs to be authenticated. Group authentication and verification ensures anonymity and conditional privacy. A new scheme for cluster formation in VANET has been discussed in this paper. RSA algorithm was used for vehicle authentication. Cyclic group concept was used to select the cluster heads for each cluster. Members of the cluster were selected using Euler’s totient function. VANET was successfully implemented in MATLAB. MATLAB is an interactive programming language developed by MathWorks. The results were recorded and analysed based on different parameters. Graphs were generated to view the variations.

6. FUTURE SCOPE

Further work will involve generation of short signature to perform group message signing and verification i,e group authentication of messages that are being sent between vehicles to communicate with one another.

7. REFERENCES

[1] Ahren Studer, f. b. 2009. Flexible, Extensible and Efficient VANET Authentication. *Journal of Communications and Networks* .

[2] Euler, L. 1763. Theoremata arithmetica nova methodo demonstrata. *Novi Commentarii academiae scientarum Petropolitanae* , 74-104.

[3] G.Clandriello, P. P. 2007. Efficient and Robust Pseudonymous authentication in VANET. *Workshop VANET*, (pp. 19-28).

[4] Hellman, W. D. 1976. New directions in Cryptography. *IEEE Transactions on information theory.*

[5] Hsin-Te Wu, W.-S. L.-S.-S. 2010. A Novel RSU-based Message Authentication Scheme for VANET. *International Conference on System and Network Communication.*

[6] Hui Zhu, T. L. 2013. PPAS: Privacy Preservation Authentication Scheme for VANET. *Cluster Computing* (pp. 873-886). Springer.

[7] Karuppanan, K. a. 2011. Secure Privacy and Distributed Group Authentication for VANET. *International Conference on Recent Trends in information technology.* IEEE.

[8] Lai, C.-C. L.-M. 2013. Toward a secure batch verification with group testing for VANET. *Springer.*

[9] M.Raya, J. 2007. Securing vehicular ad hoc network. *Journal of Computer Security* , 39-68.

[10] Norman, C. 2012. Finitely generated abelian groups and similarity of matrices over a field. *Springer Undergraduate Mathematics Series* , 47-51.

[11] Rongxing Lu, X. L.-H. 2008. ECPP: Efficient Conditional Privacy preservation Protocol for Securing vehicular communications . *IEEE INFOCOM.*

[12] Sherali Zeadally, R. H.-S. 2010. Vehicular ad hoc networks (VANETS): status,results, and challenges. *Springer* .

[13] Shoup, V. 2005. *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press.