International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-04, July 2019

Pseudonumous Authentication Through DGD and Puzzle-Based Co-Authentication in 5G-Vanet for Dos Attack Mitigation

[*]Inas Bellary, [#]Vaishali Bagade

[*]Student, [#]Assistant Professor, ARMIET Shahpur, Mumbai India.

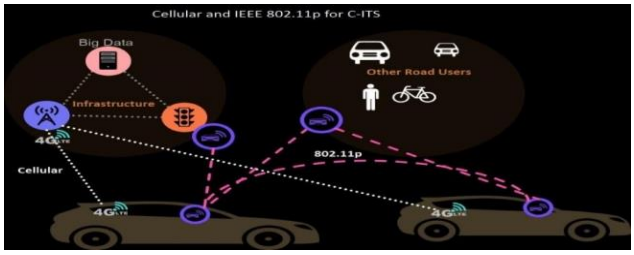
[*]inasbellary786@gmail.com, [#]vaishali.b,agade2@gmail.com

Abstract: 5G-based Vehicular Social Network (VSN) needs the vehicle's precise location while also preserving the trajectory privacy. As the VSN has the attribute of high movability and integrates the usage of multiple hops relay, the construction of the of 5G-based VSN's architecture with the Mobile Femtocell (M Femtocell) is the foundational step. Further, the introduction of the Dynamic Group Division algorithm (DGD) and exchanging pseudonyms suitable for the 5G network's dynamic property, which also meets the VSN's real-time demand is necessary. The privacy preservation is done using the DGD algorithm, which increases the chance of the exchange of pseudonym with the proposed group generating protocol, hence incorporating the pseudonym exchange protocol. Finally, we analyse how effective our proposed algorithm is using three aspects: anonymity set size, distance deviation and pseudonym entropy. The simulation results show that the protection of the vehicles' location while maintaining the privacy of the trajectory can be achieved using the DGD algorithm, which is more effective than the existing Pseudonymous Authentication through Puzzle-based Co-Authentication.

Keywords: VANET (Vehicle Ad-hoc Network), VSN (Vehicular Social Network), DGD (Dynamic Group Division algorithm), Pseudonymous Authentication, 5G, M Femtocell.

I. INTRODUCTION

Intelligent transportation systems (ITS) will support more efficient flow of the vehicular traffic, it will increase both the vehicular and pedestrian safety, and eventually autonomous driving. Wireless communications is foundation for enabling ITS. The recent advances in communications technology and systems also enable establishing reliable wireless links and networks between cars, the cars and pedestrians, and the cars and fixed infrastructure. The success of ITS will be measured in terms of how well it can scale to the ever increasing mobility scenarios and environmental conditions. This poses a stringent need for ultra-reliable and ultra-low latency communications in dense environments, where thousands of cars can be simultaneously present in a particular area, moving at different speeds and are following different trajectories. The 3rd Generation Partnership Project (3GPP) specified the long-term evolution (LTE) for providing mobile broadband services in 2008. LTE has increased its scope in a large manifold since the Release 8 (R8), which was the first release. 3GPP R12 specifies Proximity Services (ProSe) for Device-to-Device (D2D) communications. D2D is also an important mode used in mission-critical networks since it allows creating ad-hoc networks, where there is no cellular infrastructure or where there is damaged infrastructure. The next generation public safety networks will be LTE-based and will make use of UEs (user equipment) with D2D communications capabilities. The constraints and the needs of vehicular communications are different from stationary or slow moving D2D users. The high latency radiation ProSe is not appropriate for vehicular communications, where the loss or delays of packets may have severe consequences. Hence, 3GPP R14 extends the ProSe functionality by adding two new modes, Modes 3 and 4, for cellular vehicle-to-everything (C-V2X) connectivity. While Mode 3 integrates vehicle-to-infrastructure (V2I) and vehicle-to-network (V2N), the Mode 4 supports vehicle-to-vehicle (V2V) and vehicle-to-pedestrian (V2P) communications. In an alternate statement in the same context, we can reliably say that while Mode 3 makes use of the radio access network, the Mode 4 makes available to the UEs the functionality to talk with each another directly. These two C-V2X communications modes are designed to satisfy the latency requirements and accommodate high Doppler spreads and high density of vehicles. The vehicular UEs regularly broadcast short C-V2X messages, whose recipients keep changing. Hence, the conventional signalling and processing ways of authenticating and authorizing transmitters and protecting the messages are not suitable in this context and there is a need to seek alternative solutions.



Device to Device (D2D) communication & link between UEs

 DOI : 10.35291/2454-9150.2019.0366

Related work:

There are three main approaches that are extensively used to address the issue of the identification of the malware. We classify the approaches: Based on the detection techniques they employ:

(1) The Static approach analyses the application's code.

(2) The Dynamic approach inspects the behaviour of an application during the run time.

(3) The Hybrid approach is a combination of the above-mentioned methodologies. Detection Based on Static Analysis. Fuchs et al followed a particular approach for filtering the malicious applications from the benign ones. They then created ScAndroid, a tool that permitted the checking of an application during the device installation. ScAndroid exclusively extracts the security specification from the manifests that are provided along with the applications and checks if the flow of the data is consistent with a predefined set of specifications. It uses the static analysis technique for extracting the formation and takes the automated security decisions on the basis of the data flows such as gauging if it is safe to give certain accesses to an application.

II. PROPOSED METHODOLOGY AND TECHNOLOGY

In this proposed framework, we intend to deploy the DGD algorithm to secure a vehicle's location and also for protecting the trajectory in the 5G-based VSNs. To begin with, we fabricate a novel framework show with the presentation of the MFemtocell (Mobile Femtocell). Once that is achieved, the vehicles can then be strongly unified for producing a gathering in time "T" (Anonymity Duration) with the MFemtocell's assistance. The normal secrecy set size (K) and the normal separation deviation (D) of the gathering should fulfil some criterion for achieving the level of protection needed by the clients. Finally, the DGD algorithm trades the characters in a similar gathering with alias guideline. By expanding the chances to trade vehicle characters, the capacity of an aggressor to decide the genuine personality of a vehicle is prevented. Along these lines, in the light of the MFemtocell innovation, problem area idea and composite metric KDT, the issue of ensuring a vehicles' area and the direction protection is settled by augmenting the normal obscurity set size (K) and the normal separation deviation (D) for a persistent time T (Anonymity Duration) in the 5G-based VSNs.

III. DGD ALGORITHM

The DGD calculation tends to the area and direction security in the 5G-based VSNs. At the point when a vehicle sends the wellbeing message occasionally from one area, the area security is ensured. To begin with, the vehicle produces a gathering district utilizing the strategy that is presented in the Group Generating Protocol. At that point, to ensure the area protection, all vehicles trade pen names each other in a similar gathering. At the point when a vehicle is moving, area protection just as direction security ought to be considered. To powerfully produce bunch districts along the direction, the DGD calculation calls the Group Generating Protocol and Pseudonym Exchanging Protocol on the other hand.

ALGORITHM: Dynamic Group Division (DGD)

1: if (vehicle is moving)

2: Call for the Group Generating Protocol alternately;

3: Dynamically obtain group regions;

4: if (One group region is unsuccessful)

5: Go to the scheme of location privacy;

6: else

7: Call for Pseudonym Exchanging Protocol alternately;

8: end if

9: else

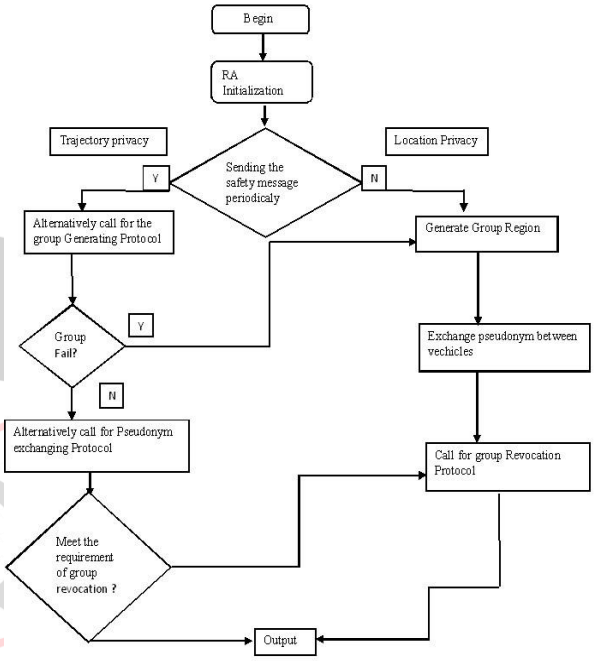
10: Generate a group region for the vehicle;

11: Exchange pseudonyms with each other;

12: end if

13: Call for Group Revocation Protocol.

IV. FLOW CHART



Group Generating Protocol

On the off chance that a vehicle is seeking access to the VSNs, the RA will approve the character of that particular vehicle. In the wake of completing framework introduction, the MFemtocell can help the vehicle naturally collaborate at a similar social/individual problem area. As per the territory size of the problem area, various cells are produced. To safeguard security, we propose the Group Generating Protocol to extend the territory of the gathering always, and afterward a gathering locale is progressively produced. Here, we clarify the principle technique of gathering creating. Initially, when a vehicle v1 enters a particular problem area, it will scan if there are other vehicles in the equivalent problem area that are emitting the Cell-Generate-Request message. In the event that another vehicle, let us assume it as v2, has started the solicitation message for cell producing, vehicle v1 will group with the cell. Something else, vehicle v1 starts the solicitation message. Inside a timestamp t_{stamp}, the cell is done and the first vehicle that sends the solicitation message turns into the Cell Leader. Second, the Cell Leader communicates the Group_Generate_Request message to locate different vehicles. At the point when the vehicle quantity in the gathering is bigger than the greatest esteem "K_{max}" (that is, $K_{ti} > K_{max}$) or the separation deviation between vehicles is bigger than the most extreme esteem "dmax" (that is, $d_{ti} > d_{max}$), the gathering is done. Something else, the zone of gathering will be reached out to discover suitable vehicles for the time t_{stamp}. Consequently, the gathering division

 DOI : 10.35291/2454-9150.2019.0366

component in the DGD calculation can all the more adequately ensure the vehicles' direction security contrasted and the protection saving plan MixGroup.

Pseudonym Exchange Protocol

For the protection of the vehicles' location while maintaining the trajectory privacy beyond the group area, the vehicles send interim safety messages with pseudo identities. The vehicles directly communicate with the Base Station. Inside of the group area, the vehicles employ group identity (GID). For ensuring that the attacker is unable to identify the vehicles' real identity, this paper increases the pseudonym exchanging opportunities. Once a vehicle enters a group region, it will continually keep exchanging pseudo identities with other vehicles till the time it leaves the group region. A condition for exchanging pseudo identities between vehicles is observed. Assume that the malicious attacker, denoted by "Pi", can probably track each vehicle. Hence, the pseudonym entropy "H" for vehicles {v1, v2,…, vk} in a group region can be expressed as follows:

The probability "Pi" and the pseudonym entropy "H" change once the vehicle's pseudo identity is changed. Hence, our paper exploits the group's entropy for exchanging the vehicles' pseudo identities for preserving privacy. The pseudo code of the Pseudonym Exchanging Protocol is shown in Algorithm 3. Here, we consider the privacy preservation of vehicle v_i in group region Gr. Before exchanging the pseudonym of vehicle "v_i", we first calculate the pseudonym entropy of the Gr, which is denoted by the symbol "H_{before}". Thus, H_{before} is the entropy before the exchanging takes place. In the valid anonymity duration "T", if "v_i" receives the message Pseudonym Exchange Request from a vehicle "v_j", we will estimate the pseudonym entropy of the group region Gr denoted by the symbol H_{after}. Of course, the vehicle v_j also belongs to the group region Gr. If the pseudonym entropy H_{after} is greater than H_{before}, the two vehicles v_i and v_j will interexchange pseudonyms. In contrast, vehicle v_i will abandon the opportunity of exchange because smaller pseudonym entropy corresponds to lower the level of privacy.

Group Revocation

When a vehicle leaves the group region, it will send a message to that particular group's Group Leader. If the lifetime of the vehicle is zero (T_{life}=0), then the vehicle will automatically apply to leave the group. When the number of vehicles in a group is less than the minimum value "K_{min}" (that is K_{ti}<K_{min}) or the distance deviation between vehicles is less than the minimum value d_{min} (that is, d_{ti}<d_{min}), we conclude that the group's existence is meaningless As a result, the group will be revoked by the RA. Algorithm 4 presents the pseudo code of the Group Revocation Protocol.

Group Revocation Protocol

Input: Group region, GID, T_{life}, K_{min}, d_{min}

Output: Resources of group

1: if (a vehicle vi∉ Group region || T_{life},<=0)

2: Initiate the message leaving_group_ request;

3: Calculate K_{ti} and d_i ;

4: if (K_{ti}<K_{min}||di

5: Group leader sends message of group revocation 6: to RA;

6: RA recovers the corresponding resources of the group;

7: end if

8: end if

V. TECHNOLOGY USED

For design our system we used MATLAB for development. MATLAB is best suited for our proposed method due to these concern:

MATLAB

The meaning of matlab is matrix laboratory. Today we need an environment, in which we need to quantify arithmetic estimation, formulation and visual graphics. For that purpose we need a language that serve high level programming with the fourth generation technology. Mathwork develop the matlab. In math's work handling of matrix is allowed; we can implement algorithm; data and function plotting; development of algorithms; user interface can be designed; programs that are written in other language can be merge, these languages include FORTRAN, C++, Java and C; it can also analyze the data; and creating different applications and models. It contains so many built in commands and functionality of mathematics which will help us in calculations of mathematical programs, plot generation and arithmetic methods can be performed. It is the very useful tool for computation of the mathematical programs.

There are several basic features in the MATLAB:

1. For arithmetic calculations, creation of applications and resolution it is used.
2. It provides collective environment in which the solving of problems, designing and repetitive study take place.
3. Statistics, filtering, arithmetic unification, linear algebra, ordinary differential equations and solving optimizations all these mathematical functions are provided by it in its library and also provide built in tools for graphical visualization of data and also provide tool for custom plots.
4. It is very efficient tool for the development of quality of codes and increasing the presentation of the interface. For graphical interface it provide in built tools.
5. It also provide tools for integrating the other language applications with the matlab based algorithms like Microsoft Excel, .Net, java and C.

M files

For the calculations, the environment of matlab is used as calculator. It is one of the powerful languages for programming and also provide connected environment for computation. Previously we discuss about how command enter in the command prompt of the matlab. We also discuss about how to writes multiple command in a single file and how this single is executed. This is like writing function into a file and then calling it.

The program file is of two types in the matlab M files:

Scripts- the program file which has .m extension is one kind of script file. In which we can write many types of commands, these commands can be executed simultaneously. These script files have some limitations like input do not accepted and nothing eil be return as the output. They are using workspace for doing any operation.

Functions - the program file which has .m extension is another kind of file called function file. Functions are those variables which accept the input and in return produce some output. All the internally define variable are like local to that function file. For the creation of ant .m file the matlab editor can be used or we can use text editor also. This section is all about the script files. Script files

 DOI : 10.35291/2454-9150.2019.0366

are those files which call multiple functions and matlab commands in sequential line. There is a very simple way to run a script file by just its name which will be type on the command line. Text editor is used to create a script file. There are two ways for the opening of the matlab editor:

- By the use of the command prompt
- By the use of the IDE

Data Types

There is no need of declaration any dimensions or data type with the statement. When the new variable is declared, it can be encountered easily and the appropriate space is allocated to it and variable is also created. In case that variable exists already then the original variable is replaced with the new one and its content is also replaced and for storage new space is also allocated if it is required.

There are 15 types of data types which are provided by this language. Every data types have some common functionality like the array or matrix type data is stored by these data types. The advantage of these data types is that they can store the array or matrix is of any length and minimum of 0 by 0. There is a table which represents the data types that are very commonly used in matlab:

Data Type	Description
int8	8-bit signed integer
uint8	8-bit unsigned integer
int16	16-bit signed integer
uint16	16-bit unsigned integer
int32	32-bit signed integer
uint32	32-bit unsigned integer
int64	64-bit signed integer
int64	64-bit unsigned integer

Describes some Data types and their description

Operators – from the name itself it suggest to do some operation, for logical calculations or perform mathematical operations this symbol is used which gives orders to the compiler to compile them. The basic designing of matlab is to operate the arrays or matrices primarily. Both non scalar and scalar data are operated by these operators.

- Relation Operators
- Logical Operators
- Bitwise Operators
- Set Operators
- Arithmetic Operators

MATLAB allows different types of arithmetic operations:

- Matrix arithmetic operations
- Array arithmetic operations

Vectors

One dimensional array is called vectors of numbers. There are two types of vectors in matlab:

Row Vectors: This type of vector is created when the set of data or element are bound by square brackets, for unlimited elements we are using comma or space.

Column Vectors: This type of vector is created when the set of data or element are bound by square brackets, for unlimited elements we are using semicolon.

VI. IMPLEMENTATIONS

Implementation Procedure:

We conduct extensive simulations and evaluate the performance and effectiveness of our proposed DGD algorithm for Vanet. We first describe the simulation environment for the city and suburban scenarios. The simulation results from three aspects (anonymity set size *K*, distance deviation *D* and pseudonym entropy *H*). Eventually, using the results of the simulation, we conclude that our proposed DGD algorithm can effectively protect the location while maintaining the trajectory privacy in 5G-based VSNs. For the further simplification of our experiment, we assume that a vehicle is in the social zone and sending a request message for the generation of the group. We analyse the location privacy in the city scenario and suburban scenario from two aspects: anonymity set size and distance deviation.

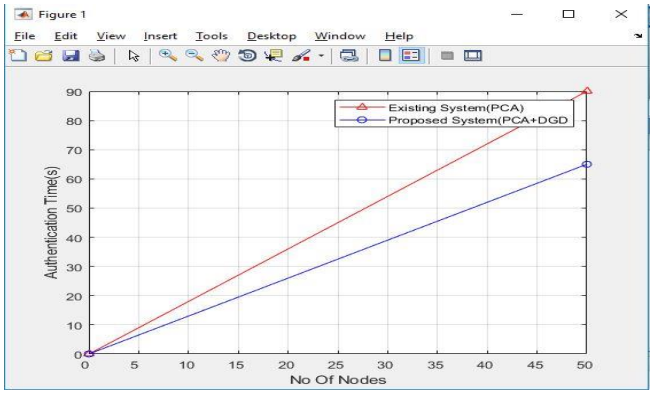
Simulation Environment

Vehicle Speed	30 km/h
Vehicle density	0.3 v/m for city scenario
Vehicle density	0.2 v/m for suburban scenario
Anonymity Duration	600 s
kmin	35
Dmin	600 m
kmax	50
dmax	750 m

Simulation Parameters

Description

This graph compares the time between the DGD and existing algorithm in a single group region. From the figure, we can see that the authentication rate of DGD algorithm is faster than the existing algorithm. The DGD algorithm achieves the authentication time about t=60s, while the existing algorithm is 90s. Thus, this further proves that our proposed DGD algorithm has faster response speed while still reliably protecting the privacy of the vehicle's location.



Comparison Graph between Current Technique and Previous Technique

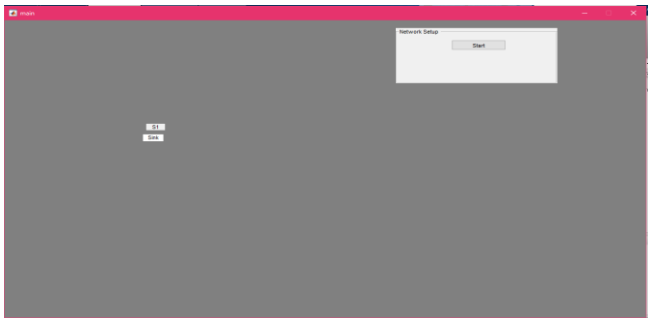
In our system model, we design an efficient Dynamic Group Division (DGD) algorithm for protecting the vehicles' location while still keeping the trajectory privacy intact. The DGD algorithm includes four stages: system initialization, group

 DOI : 10.35291/2454-9150.2019.0366

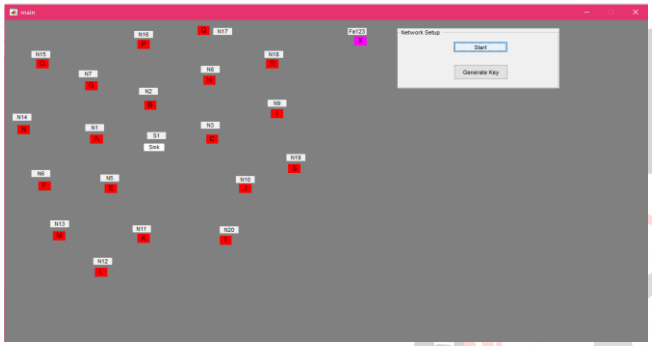
generating, pseudonyms exchange, and group cancellation. Through the simulations we show that our algorithm reduces the time delay compared to existing solutions for generating group region and effectively protects users' location and trajectory privacy in 5G-based VSN.

VII. RESULT (SNAPSHOT OF OUTPUT)

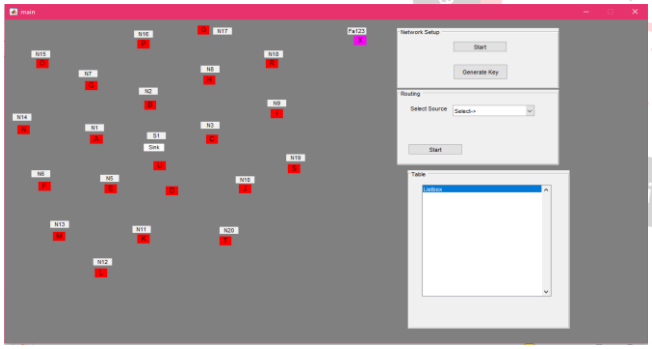
Step1: Create GUI



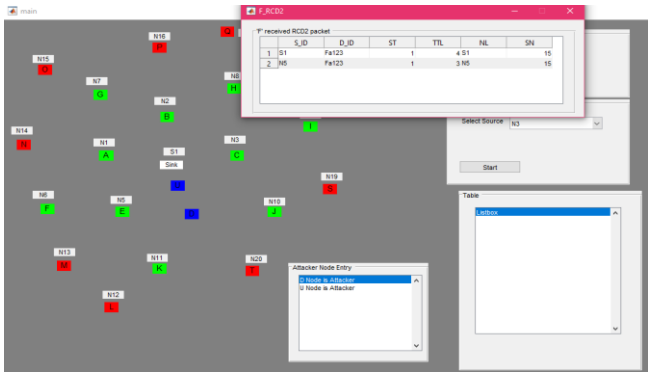
Step 2: Vehicle Initialization



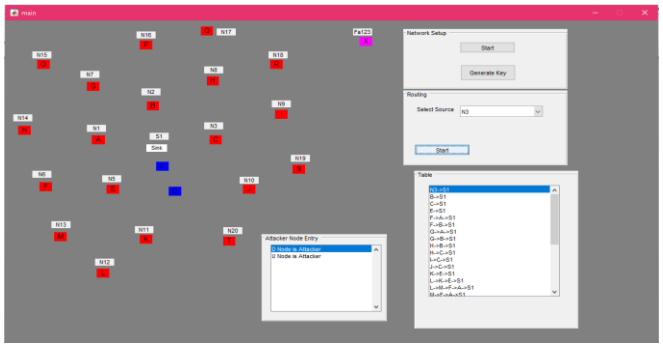
Step3: Key generation



Step4: Routing



Step 5: Final output routing completed



VIII. APPLICATION OF THE TECHNIQUES

A] The main purpose of the DGD algorithm is the security of the vehicle's location and trajectory protection in 5G-based VSNs. The PCA scheme can provide the capacity of resisting the DoS attacks against pseudonymous authentication and improving the efficiency of certificates verification in 5G-VANET. Hence, the Mix Group statically produces a gathering locale. Expect that a noxious assailant has participated in the gathering locale. At that point, he/she will always trade pen names with different vehicles situated in a similar gathering area and will continue endeavouring trading pen names, leaving the gathering district. The vindictive assailant can draw the framework of the gathering area. By coordinating gathering locales with the guide (e.g., Google Maps), the assailant learns the directions of vehicles with an on the off chance that it can also access other data.

B] In this paper, C-V2X is introduced for safety and non-safety related applications. The safety applications include the dissemination of accidents and sudden braking. The non-safety applications enable operational and resource efficiencies, among others, by providing relevant information about the road status, traffic lights, and so forth. Both the types of applications require reliable and timely reception of messages that are confidential and integrity protected. Hence, security is another important requirement for C-V2X and comprises of a difficult research problem due to the strict resource constraints and the dynamics of C-V2X systems and applications. The messages emitted from C-V2X are short and are regularly broadcast from vehicular UEs, whose recipients keep continually changing. Hence, the traditional signalling and processing procedures to authenticate and authorize transmitters and protect messages are not suitable in this context and alternative solutions need to be sought.

C] Warning Message Transfer such as Attacker alert message will exchange by vehicle and co-operate to help other vehicles. Although reliability and latency would be of major concern, it may automate things like every vehicle will get notified, and the server will provide the alert message to each vehicle in the cluster. Similarly, the alarm light will also be generated. Hence, all these things will be done by DGD Algorithm and PCA technique.

IX. LIMITATIONS

1. The limitation of wireless communication and computing capability of drones, the application of UAV is getting increasingly complicated, especially for security and privacy issues.

2. Categorised threat models on the drone-assisted public safety network, in four categories, namely, attacks on confidentiality,

 DOI : 10.35291/2454-9150.2019.0366

attacks on integrity, attacks on availability, and attacks on authenticity.

3. One possible future direction is to develop a privacy preserving schemes for UAV systems in 5G heterogeneous communication environment.

X. FUTURE SCOPE

1. The future research about authentication and privacy-preserving schemes, which are:
a. Fog paradigm-based 5G radio access network,
b. 5G small cell-based smart grids,
c. SDN/NFV based architecture in 5G scenarios,
d. Dataset for intrusion detection in 5G scenarios, 7
e. UAV systems in 5G environment
f. 5G small cell based vehicular crowd sensing,
By using DGD Algorithm and including existing PCA technique increased the protections, high security and safety.

2. The efficient scheduling scheme and energy-efficient networking is some of the significant challenges.

3. Security becomes a big challenge for VANET efficiency applications. Validation is becoming more challenging for assessment of VANET performance in realistic scenarios.

4. This can be slightly resolved in some cases by performing field operation Test (FOT). And Vehicular Cloud Computing (VCC) is a new technological shifting, which takes advantage of cloud computing to serve the drivers of VANETs with a pay as you go model.

5. Thus, the objectives of VCC are to provide several computational services at low cost to the vehicle drivers; to minimize traffic congestion, accidents, travel time and environmental pollution; and to ensure uses of low energy and real time services of software, platforms, and infrastructure with QOS drivers.

XI. CONCLUSIONS

In this report we have considered the issue of ensuring area and direction protection in 5G-based VSN. To powerfully partition the gathering area and fulfil the high real time requirement of the clients, we suggest the framework model of 5Gbased Vehicular Social Network applying the innovation of MFemtocell. In our proposed framework demonstrate, we plan a proficient Dynamic Group Division (DGD) calculation for ensuring vehicles' area and direction protection. The DGD calculation incorporates four phases: framework instatement, gathering producing, nom de plumes, and gathering crossing out. Through the reproductions, we demonstrate that our calculation diminishes the time delay contrasted with existing answers for creating gather district and adequately ensures clients' area and direction protection in 5G-based VSN.

ACKNOWLEDGMENT

I would like to acknowledge and extend our heartfelt gratitude to University of Mumbai and all my Institute people who have been associated with this research work and have helped me with it thus making it a worthwhile experience.

REFERENCES

[1] Gartner Inc, *The Internet of Things Is a Revolution Waiting to Happen*, 30 April 2015.

[2] McKinsey, Global Institute, *Unlocking the Potential of the Internet of Things*, June 2015.

[3] *Hitachi Ltd., Information and Control Systems – Open Innovation Achieved through Symbiotic Autonomous Decentralization*, Hitachi Review Vol.65 (2016), No.5, 2016.

[4] P. Li, J. Li, Z. Huang, T. Li, C. Z. Gao, S. M. Yiu, and K. Chen, *"Multi-key privacy-preserving deep learning in cloud computing,"* Future Generation Computer Systems, vol. 74, no. C, pp. 76–85, 2017.

[5] 5GAA, *"The case for cellular v2x for safety and cooperative driving,"* 2016, accessed November 1, 2017.

[6] Qualcomm, *"Qualcomm announces ground breaking cellular-v2x solution to support automotive road safety, helping to pave a path for the future of autonomous driving".*

[7] Saini R., Khari, M, *"Defining Malicious Behaviour of a Node and its Defensive Techniques in Ad Hoc Networks. Journal of Smart Sensors and Ad-hoc Networks"* (IJSSAN). 2011;1:18–21.

[8] L. He and W. T. Zhu, *"Mitigating dos attacks against signature-based authentication in vanets,"* in IEEE International Conference on Computer Science and Automation Engineering, 2012, pp. 261–265.

 DOI : 10.35291/2454-9150.2019.0366