A Novel Clustering based Approach with Hybrid Cryptography to Secure Vehicular Adhoc Network

Amandeep Singh
M.Tech Scholar,
IKG Punjab Technical University,
Regional Center, ACET ,Amritsar

Sandeep Kad
Associate Professor,
Department of Computer Science,
ACET, Amritsar

ABSTRACT
VANETs (vehicular specially appointed systems) are developing as another system environment for wise transportation frameworks. Nowdays , security conservation is most critical viewpoint in vehicular specially appointed systems as vehicular correspondence is powerless against assaults. Assailants might misuse VANETs to send sham data to trick different vehicles which prompts significant issues. Already such a large number of procedures were utilized to give security. However, the issue is that a large portion of the hubs are in the same group and as a result of that there is blockage in that bunch just furthermore a straightforward information encryption is utilized which split effectively. Presently, to conquer this issue this work has a centre to utilize a novel bunching calculation called constraining part hub grouping (LmC) calculation to restrain the quantity of part hubs for every group head by utilizing a limit esteem. This grouping approach chooses a bunch head in light of another cost capacity which considers the remaining battery level, vitality utilization and separation to the base station. At that point will actualize a half breed cryptography in view of Diffie-Hellman and AES for secure correspondence. This methodology gives an enhanced state security than others.

Keywords
LmC, Clustering, CA, CH, AES, Diffie-Hellman.

1. INTRODUCTION
The coming of ad hoc Wi-Fi social media is probably one of the most important improvements in Wi-Fi social media and telecoms in the last several years. While the analysis into this place has started as a result of the immediate needs of the Department of Defence (DoD) in the USA for army fight functions in aggressive areas, the program areas have since expanded extremely and have extended to consist of the complete place of indicator systems as well. Nevertheless, it is reasonable to say that the large of the analysis in ad hoc systems has remained targeted on army programs with few professional programs that seemed practical later on[1]. This image has modified considerably in the last 5 years or so with the coming of the vehicle market displaying attention later on of Vehicle Ad Hoc Networks, mainly for protection programs. Indeed, this is probably the greatest new professional program of ad hoc systems with real and tangible programs (such as safety) driving the goal of the actual technological innovation. With the growth in the area of Wi-Fi emails, ITS programs are designed based on car-to-car interaction requirements such as

Wireless Access in Vehicle Environments (WAVE) and Dedicated Short Range Communications (DSRC). WAVE and DSRC requirements are described in IEEE 1609.1-4 and 802.11p respectively. The fact that FCC has assigned dedicated 75 MHz regularity variety in the range of products 5.85 GHz to 5.925 GHz to be used only for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) interaction.

Vehicle ad hoc systems are increasing new technological innovation to merge the performance of new Wi-Fi systems with automobiles. The key technicalities of a VANET are Wi-Fi on board device (OBU), the roadside unit (RSU) and the verification server (AS). OBUs are set up in automobiles to give Wi-Fi interaction ability, while RSUs are implemented on crossing points or locations as a facility to provide information or internet connection for automobiles within their radio coverage[5].

1.1. Security Issues In Vanet
Among each one of the troubles of the VANET, security got less thought thusly. VANET packages contains life fundamental information therefore guarantee that these groups are not implanted or adjusted by the attacker; in like way the commitment of drivers should in like manner be set up that they light up the movement environment viably and within time. These security issues don't care for general correspondence framework. The measure of framework, flexibility, geographic significance thus on makes the use troublesome and unmistakable from other framework security

The troubles of security must be considered in the midst of the setup of VANET designing, security traditions, cryptographic computation et cetera. The going with summary shows some security challenges [6]:

- Real time Constraint
- Data Consistency Liability
- Low tolerance for error
- Key Distribution
- Incentives
- High Mobility
- Low complexity security algorithms
- Transport protocol choice

1.2. Security Requirements In Vanet
VANET must fulfil some security prerequisites before they are sent. A security framework in VANET ought to fulfil the accompanying prerequisites [7]:

- Authentication
- Availability
- Non-Repudiation

1.3. Lmc Clustering In Vanet

Clustering in VANETs [8] is defined as a process of organizing nodes into different groups where nodes are similar in some way. In this work, LmC Clustering algorithm is used which were used in sensor networks only.. LmC [9] is Limited member node Clustering and in this cluster head selection is based on the cost function.

1.4. AES Encryption In Vanets

AES has a settled piece size of 128 bits and a key size of 128, 192, or 256 bits, while it can be resolved with square and key sizes in any various of 32 bits, with no less than 128 bits and a most great of 256 bits. Expecting one byte squares with 8 bits, the adjusted piece size of 128 bits is 128/8 = 16 bytes. AES takes a shot at a 4×4 bunch of bytes, termed the state (adjustments of Rijndael with a greater square size have additional segments in the state). The AES figure is shown as different redundancies of progress modifies that change over the data plain-message into the last yield of ciphertext [10]. Each round contains a couple taking care of steps including one that depends on upon the encryption key. A course of action of inverse rounds is associated with change consider substance at the end of the day along with the main plain-message using the same encryption key.

1.5. Diffie Hellman In Vanets

Diffie–Hellman key exchange (D–H) is a specific methodology for exchanging cryptographic keys. It is a standout amongst the most dependable conventional representations of key exchange executed within the field of cryptography. The Diffie–Hellman [11] key exchange procedure grants two social occasions that have no prior learning of each other to commonly set up a typical puzzle key over a flimsy correspondences channel. This key can then be used to encode following exchanges using a symmetric key figure. Diffie–Hellman key understanding itself is a mysterious (non-validated) key-assertion convention; it gives the premise to an assortment of confirmed conventions, and is utilized to give immaculate forward mystery in Transport Layer Security's fleetin.

2. PROPOSED WORK

VANETs (vehicular specially appointed systems) are rising as another system environment for canny transportation frameworks. Nowadays, security protection is most vital angle in vehicular specially appointed systems as vehicular correspondence is powerless against assaults. Assailants might abuse VANETs to send sham data to betray different vehicles which prompts difficult issues. In this paper, we portray a progressed Secure plan in light of Clustering and Key Distribution (SCKD) among individuals and group heads in VANET. The SCKD[12] is a coordination based calculation in which hubs are situated inside various bunches and their group heads are looked over trusty hubs. For a safe end-to-end correspondence, our plan conveys the intermediary signature, blind intermediary signature, hashed message validation code, and symmetric cryptography. Results demonstrate that our plan jam security prerequisites including validation, classification, information uprightness, non-disavowal, and unforgeability. Following the expense and time calculation of key era and dispersion diminishes by SCKD contrasted and different calculations, our calculation will be appropriate for VANETs. In this work, hubs dispersed in bunch as indicated by their extent or area. Here issue is if most elevated include of hubs are the same area run then every one of that hubs in the same bunch and on account of that there is clog in that group just and a basic information encryption is utilized which split effortlessly.

Presently, to conquer this issue this work has an attention on, to utilize a novel grouping calculation called constraining part hub bunching (LmC) calculation to restrict the quantity of part hubs for every group head by utilizing an edge esteem. This grouping approach chooses a bunch head taking into account another cost capacity which considers the leftover battery level, vitality utilization and separation to the base station. At that point will execute a cross breed cryptography taking into account Diffie-Hellman and AES to accomplish the accompanying targets.

2.1. Proposed Flow Of Work

Presently proposed work has a centre to execute a novel security system with restricting part hub bunching (LmC) calculation to confine the quantity of part hubs for every group head by utilizing limit esteem. This bunching approach chooses a group head taking into account another cost capacity which considers the lingering battery level, vitality utilization and separation to the base station. Then will implement a hybrid cryptography based on Diffie-Hellman & AES for secure communication. The proposed flow of operation:

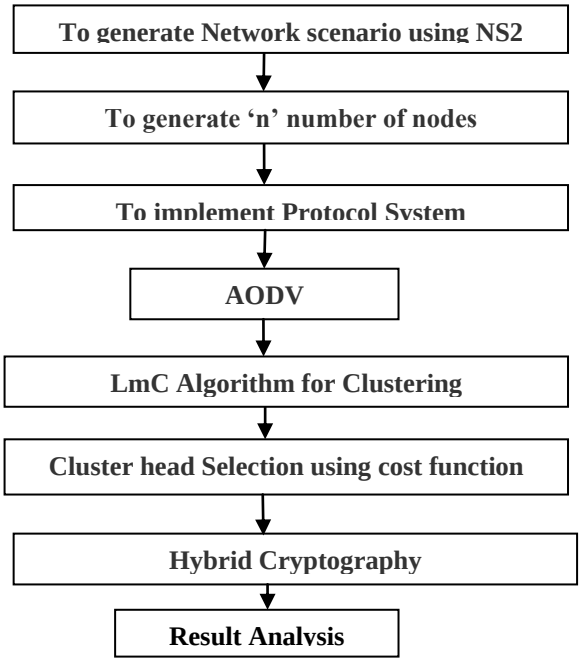

fig 1. Flow of Work

3. METHODOLOGY

The main focus of this proposed work is to enhance the security. To achieve this objective following steps has been considered in the work:

Step 1: In this step the certification authority firstly selects cluster heads from different clusters. These cluster heads are selected on the bases of trusted nodes and through previous communication. Every clusters have its own cluster head i.e. number of cluster heads depends on the number of clusters. Clusters are made by LmC algorithm that is Limited member node clustering algorithm.

Step 2: Now CA provides a unique master key to each cluster head. Each cluster head distributes unique key to every node.

Step 3: Once each node receive their respective key they submit it to certification authority. Then CA saves the keys in the database as during the transfer it checks the keys.

Step 4: Now whenever a communication is to be made between the source and destination. When the route request is made source node sends the request to its neighbouring nodes along with the keys. Then its neighbour to their neighbour till it reaches the destination. Once the destination is reached it send the route reply along the keys. Through this the most secured and optimized path is selected for communication.

Step 5: Finally once the path is selected the data transmission begins.

3.1.Simulation Analysis

Simulation is a very important and integral part of technology. Simulation can be performed to different applications and for different purposes. Computerized simulations are performed to interpret the behavior or the performance of any system. Different values are used to measure the performance of any system during the simulation. Many Natural systems are also analyzed using the simulations performed using the computers. The main applications in which the simulation is performed include social science, chemistry, economics, biology, finance and physics. Simulation [13] is also widely used in all types of Engineering such as Mechanical, Civil, Structural and computer engineering. The applications for simulation are increasing very rapidly and simulation is becoming part of network traffic control design systems as well.

3.2.Network Simulation And Simulator

Simulation is very important in the research area of computer and communication. The communication between all the network components or nodes can be studied using the formulas and simulations. Various types of components to be simulates can include end users, routers, switches, servers, data centres, link between components and communication packets. Mathematical formulas are used in the simulation to understand the behavior. Observations are done during the simulation before the actual deployment of the network. Series of simulation are done in order to identify the response of the network components and to understand the network protocol behavior. The simulation tests are performed in offline mode [14]. The networks parameters are updated and changed during the simulation o identify the end result that can be achieved by the use of given setup in a network. The results from simulation test help to identify the complete communication across the network.

3.3. Network Simulator 2

Network Simulation (Version 2), commonly known as NS2, is simply a meeting motivated simulator device that has shown useful in learning the powerful characteristics of interaction systems. Simulation of wired as well as Wi-Fi network features and methods (e.g., redirecting methods, TCP, UDP) can be done using NS2. In common, NS2 provides customers with a way of specifying such network methods and replicating their corresponding actions. Due to its versatility and flip characteristics, NS2 has obtained continuous reputation in the social media analysis team since its beginning in 1989 [11]. Ever since, several radical changes and modifications have noticeable the increasing adulthood of the device, thanks to significant efforts from the gamers in the area. Among these are the School of Florida and Cornell School who designed the REAL network simulator, the base which NS is based on. Since 1995 the Protection Innovative Research Tasks Organization (DARPA) reinforced growth of NS through the Exclusive Internetwork Test bed (VINT) venture [8].Currently the Nationwide Technology Foundation (NSF) has signed up with the drive in growth. Last but not the least, the number of scientists and designers in the team are regularly working to keep NS2 powerful and flexible. Especially, NS-2 resources are used to produce the network situation and traffic design resolved in this plan. Developing network to do some real tests is the best way for learning about interaction in internet. However, establishing a network is not simple and expensive. For this reason, an online network offered by network simulator is used for analysis in only one computer. Exclusively, NS2 which is free and simple to use is the popular all over the world. NS2 use Tcl terminology for creating simulator situation information file (for example, example.tcl). System topology, transmitting time, uses method etc... Are described in situation information file. If these situation information files are performing, the simulator outcome will be outcome to out.tr and out.nam information file. Out.tr all the information about interaction is published in this information file. This information file is known as track information file. Out.nam contains the information for computer animation of the analysis outcome. This information file can be perform by Nam, an computer animation software [9].

3.4. Simulation Parameters

The simulation has been conducted using NS-2.35. In this simulation had taken the ASSD strategy as base. We have measured the throughput, bundle distribution rate and End to End wait for unclear then the same process is recurring inherited criteria and then for multiple of unclear and inherited criteria i.e. our suggested criteria. The simulation outcome reveals that our suggested criteria give the better efficiency in requirements of throughput bundle distribution rate and end to end wait. So will evaluate the current criteria with the suggested criteria[8].

Simulation has been conducted by taking the above mentioned simulation factors. The track information has been produced by replicating the situation and with the help of XGRAPH and AWK information outcomes are developed.

Table 1. Simulation Setup

Parameter	**Value**
Channel Type	Channel/Wireless Channel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface queue type	CMUPriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Max packet in ifq	500
Number of nodes	100

Protocol	AODV
X axis distance	3000
Y axis distance	3000
Initial energy in Joules	100

3.5.Simulation Analysis

Step 1: In this step shown in fig 2, the certification authority firstly selects cluster heads from different clusters. These cluster heads are selected on the bases of trusted nodes and through previous communication. Every clusters have its own cluster head i.e. number of cluster heads depends on the number of clusters. Clusters are made by LmC algorithm that is Limited member node clustering algorithm.

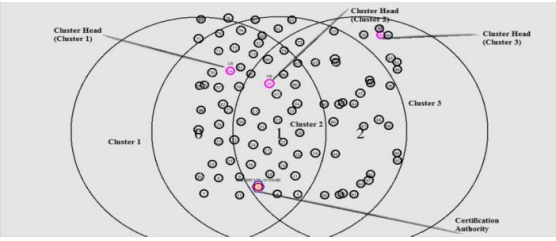

Fig2. Clustering in Novel Architecture

Step 2: Now CA provides a unique master key to each cluster head. Each cluster head distributes unique key to every node. Once each node receive their respective key they submit it to certification authority. Then CA saves the keys in the database as during the transfer it checks the keys. Now whenever a communication is to be made between the source and destination. When the route request is made source node sends the request to its neighbouring nodes along with the keys. Then its neighbour to their neighbour till it reaches the destination. Once the destination is reached it send the route reply along the the keys. Through this the most secured and optimized path is selected for communication.

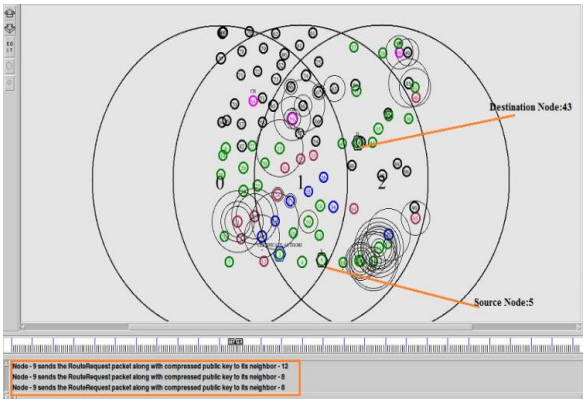

Fig3. Secure selection of nodes for transmission

Step 3: Finally once the path is selected the data transmission begins.

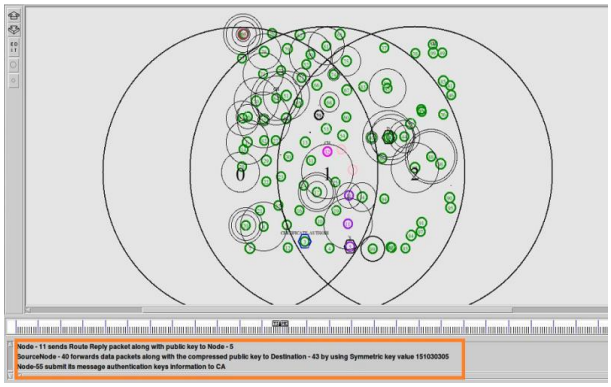

Fig4. Transmission in Novel Architecture

4. RESULT ANALYSIS

In this work, for analyze the results and behaviour of simulation computation time is calculated for key generation and key distribution. This time can be calculated for both that is communication within cluster (same cluster) and between different clusters. Computation time for key generation is defined as a total time for generating key using AES and Diffie Hellman Algorithm. Computation time for key distribution is the time taken by certification authority to distribute keys to nodes present in the cluster through their cluster head.

Fig 5 shows Computation Time for Key generation and distribution in between two different clusters. It shows that the enhanced approach takes less time for key generation and distribution when communication takes place in between two different clusters.

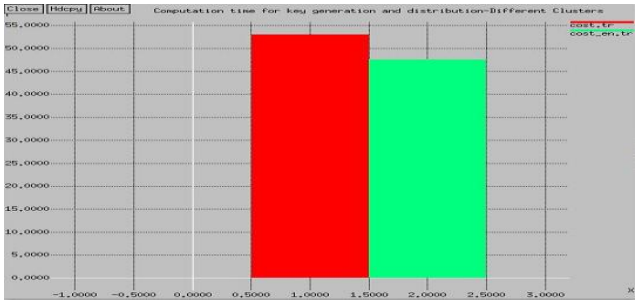

Fig5. Computation Time for Key generation and distribution-different clusters

Fig 6 shows Computation Time for Key generation and distribution within two same clusters. It shows that the enhanced approach takes less time for key generation and distribution when communication takes place within the cluster.

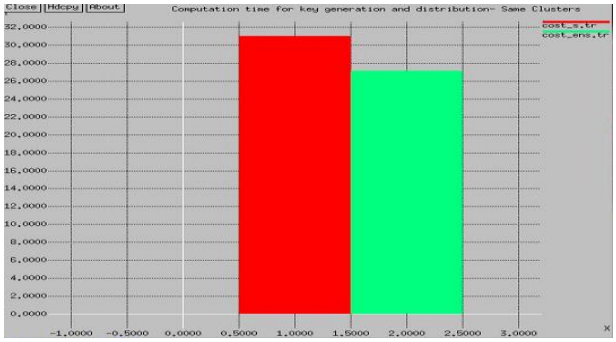

Fig6. Computation Time for Key generation and distribution-same clusters

5. CONCLUSION

There is undoubtedly Vehicular frameworks (VANETs) are a creating research territory with a broad number of usage cases. Foreseen applications consolidate wellbeing applications, infotainment administrations, and so on. VANETs associate vehicle into gigantic portable impromptu system offer information on a greater scale. The properties of VANET stance both challenges and opportunities in fulfilling security targets. Offering security to VANET is fundamental regarding giving customer acceptance, secrecy, genuineness and insurance of data. Indeed, even after various strategies being actualized time to time, security still remains a noteworthy issue. So, this work gives a novel solution to the security issue in which a bunching calculation called constraining part hub grouping (LmC) calculation to restrain the quantity of part hubs for every group head by utilizing limit esteem. This grouping approach chooses a bunch head in light of another cost capacity which considers the remaining battery level, vitality utilization and separation to the base station. At that point will actualize a half breed cryptography in view of Diffie-Hellman and AES for secure correspondence. Results shows that this methodology gives an enhanced state security than others also this approach reduced the computation time required for generation an distribution of keys.

6. REFERENCES

[1] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, Hui Li, Weidong Zhang, and Zan Li, "Privacy-preserving authentication based on group signature for VANETs," *2013 IEEE Glob. Commun. Conf.*, pp. 4609–4614, 2013.

[2] S. Bitam, A. Mellouk, and S. Zeadally, "HyBR: A Hybrid Bio-inspired Bee swarm Routing protocol for safety applications in Vehicular Ad hoc NETworks (VANETs)," *J. Syst. Archit.*, vol. 59, no. 10 PART B, pp. 953–957, 2013.

[3] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *CSAE 2012 - Proceedings, 2012 IEEE Int. Conf. Comput. Sci. Autom. Eng.*, vol. 3, pp. 261–265, 2012.

[4] J. Petit, M. Feiri, and F. Kargl, "Spoofed data detection in VANETs using dynamic thresholds," *IEEE Veh. Netw. Conf. VNC*, pp. 25–32, 2011.

[5] K. Verma, H. Hasbullah, and H. K. Saini, "Reference broadcast synchronization-based prevention to DoS attacks in VANET," *2014 7th Int. Conf. Contemp. Comput. IC3 2014*, pp. 270–275, 2014.

[6] L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 605–615, 2011.

[7] O. Chakroun and S. Cherkaoui, "Overhead-free congestion control and data dissemination for 802.11p VANETs," *Veh. Commun.*, vol. 1, no. 3, pp. 123–133, 2014.

[8] R. S. Bali, N. Kumar, and J. J. P. C. Rodrigues, "Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions," *Veh. Commun.*, vol. 1, no. 3, pp. 134–152, 2014.

[9] M. Becker, A. Gupta, M. Marot, and H. Singh, "Improving Clustering Techniques in Wireless Sensor Networks Using Thinning Process," *Perform. Eval. Comput. Commun. Syst. Milestones Futur. Challenges*, 2010.

[10] Y. A. Suryawanshi, A. Kapur, and M. D. Chawhan, "Analysis of Symmetric Key Cryptosystem in VANET," vol. 7, no. 2, pp. 3–7, 2012.

[11] S. Neelavathy Pari, S. Jayapal, and S. Duraisamy, "A trust system in manet with secure key authentication mechanism," *Int. Conf. Recent Trends Inf. Technol. ICRTIT 2012*, pp. 261–265, 2012.

[12] A. Katal, "A Cluster Based Detection and Prevention Mechanism against Novel Datagram Chunk Dropping Attack in MANET Multimedia Transmission," no. Ict, pp. 479–484, 2013.

[13] I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," *2013 IEEE Globecom Work. GC Wkshps 2013*, pp. 1344–1349, 2013.

[14] J. Sun and Y. Fang, "A defense technique against misbehavior in VANETs based on threshold authentication," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, 2008.

[15] C. Song, M. Liu, H. G. Gong, G. H. Chen, and J. N. Cao, "Utilizing the dropped packets for data delivery in VANETs," *J. China Univ. Posts Telecommun.*, vol. 20, no. 3, pp. 48–52, 2013.