International Journal of Innovative Research in Technology & Science
ISSN: 2321-1156 Volume VII Issue VI, November 2019

A Secure Vehicular Communication Using Road Side Unit Trust Management Scheme

Tejal Maheshwari, Department of computer science, Vindhya Institute of Technology & Science; tejal8644@gmail.com;

Abstract— the responsibility of every vehicle is to forward the traffic status to requester vehicles. As same as MANET due to open medium security is always the major concern in VANET. The attacker vehicle drops a huge amount of data packets that contain the information of traffic status. In this paper, we proposed the secure VANET communication in the presence of RSU. RSU identified the attacker vehicles by that unusual interference in communication. The RSU collects the information from vehicles and forwarded it to other vehicles or other RSU. The proposed Attack Prevention algorithm is applied to RSU to recognize the attacker vehicle activities. The RSU after identified it block their functionality of communication. We assume that RSUs are deployed along the highway which is at least several kilometers far from each other. On the highway, maybe some vehicles travel faster or slower than average, but we assume the majority of vehicles travel in normal or similar velocities. The aim of this research is to providing security against malicious attacks, to allow new proposed models to build their work on solid realistic models against packet dropping attack. The performance of the proposed secure algorithm is compared with the old Base-line scheme and ART scheme in VANET. In this proposed scheme, vehicles obtain traffic data when they pass by a roadside unit (RSU) and then share the data after They travel out of the RSU's coverage. The performance of the proposed scheme is better than an existing scheme in terms of providing security and overcome from the problem of congestion to manage traffic in a network.

Keywords: VANET, RSU, Attack, congestion, Road map.

1. INTRODUCTION

In the past decade, the growing need for increased safety, efficiency and congestion-free vehicular communication that promoted to vehicle manufacturers to design semi-automated vehicles integrated with the wireless communication and devices into the vehicles. The world's leading vehicle manufacturers have been and are still engaged in continuous competitions to present for today's sophisticated drivers, vehicles that gratify their demands. This has lead to an outstanding advancement and development of the vehicular manufacturing industry and has primarily contributed to the augmentation of the twenty-first century's vehicle with an appealing and intelligent personality. Particularly, the marriage of information technology to the transport infrastructure gave birth to a novel communication paradigm known as Vehicular Networking. More precisely, being equipped with computerized modules and wireless communication devices, are the majority of today's vehicles qualify to act as typical mobile network nodes that can communicate with each other. Besides, these vehicles can as well communicate with other wireless units such as routers, access points, base stations and data ports that are arbitrarily deployed at fixed locations along roadways. These fixed units are referred to as Stationary Roadside Units (SRUs) [11].

Ephemeral and self-organized networks can be formed. Such networks are known as Vehicular Networks and constitute the core of the latitudinarian Intelligent Transportation System (ITS) that embraces a wide variety of applications including but not limited to: traffic management, passenger and road safety, environment monitoring and road surveillance, hot-spot guidance, on the fly Internet access, remote region connectivity, information sharing and dissemination, peer-to-peer services and so forth. In this paper resolve the problem of security, safety, and congestion from a vehicular ad-hoc network that's controlled by roadside unit. Roadside unit (RSUs) monitor, control, and provide safety as well as security to vehicles under the radio range of RSUs and road map of VANET.

II.LITERATURE SURVEY

This section describes the existing work that provides secure and congestion-free communication against VANET. Sudha Dwivedi, Rajni Dubey, Nirupama Tiwari [1]"Trust-Based Scenario using AES Encryption in VANET "in this title we discuss Security is the main concern of any other network because of if attacks apply in networks than users suffer and quality of service is down when we talk about VANET which is highly moveable or infrastructure of VANET change frequently in this network security is main concern because if its flexible and secure passengers feel convenient to travel. Trust is the most important area, to build trust between vehicles we apply behavior-based technique for passive attack we use AES encryption.

Wenjia Li, Member, IEEE, and Housing Song, Senior Member, IEEE[2] “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks” In this title, an attack-resistant trust management scheme (ART) is proposed for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Especially, data trust is evaluated based on the data sensed and collected from multiple vehicles;

node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. The effectiveness and efficiency of the proposed ART scheme is validated through extensive experiments. The proposed trust management theme applies to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.

Gaikwad Priti G., Nilam Patil [3] "Survey on Vehicular Ad Hoc Networks Security" in this title is to give an overview of the vehicular ad hoc networks. We discuss recent advances in communication technology are enabling the implementation of different types of network in various environments. One such network is Vehicular Ad hoc Network (VANET). It is a challenging subclass of Mobile Ad hoc Network (MANET) which enables intelligent communication among vehicles and also between vehicle and roadside infrastructures. It is a promising approach for the Intelligent Transport System (ITS). There are many challenges to be addressed when employing VANET. It has a very high dynamic topology and constrained mobility which makes the traditional MANET protocols unsuitable for VANET.

Ayana Santhosh, Bini babu, Jain maria, Ashly Angel [4] "Secured Data Transmission Method for Van Networks" in this title VANET, vehicular ad-hoc network provides wireless communication between vehicles. It will help people to travel safely. In the existing system, VANET having some threats like nonrepudiation, access control, data trust, data verification. So to provide data trust and node trust a new scheme is introduced called ART, Attack Resistant Trust Management scheme. This scheme will calculate the trustworthiness of data, also finds the malicious attacks from other devices. In our proposed work we are extending the idea of ART, by introducing a method to provide data verification. Data verification is the process in which different types of data are checked for accuracy and inconsistencies after data migration is done. It helps to determine whether data was accurately translated when data is transferred from one source to another, is complete, and supports processes in the new system. This can be implemented by using an algorithm namely, advanced encryption standard.

Divya A-C, K Vyshnavi, Kusuma N, Revathy S [5] "Increasing Trustworthiness in Data Transfer of Vehicular Ad Hoc Networks" in this title we focus Vehicular ad-hoc network (VANETs) is a type of a network that is created from the concept of cars for a specific need or situation. It was shown that vehicle to vehicle and vehicle to roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services. VANETs are used to transform the way vehicles travel from the creation of a safe and secure exchange and use of information. VANETs are vulnerable to security threats due to increasing reliance on communication, computing and control technologies.

Arya Chandran & Ajay [6] "VANET Based Communication Scheme in Network Environment" in this title we discuss The Vehicular Ad-Hoc Network (VANET) is an application derived from the MANET (Mobile Ad-Hoc Network) is a current research topic in intelligence transport system. VANET provides wireless communication between the vehicles which help in road safety application such as traffic and accident. So the security of the VANET is an important factor. Different techniques exist for evaluation of the security of VANET. In ART: An attack-resistant trust management, the existing system provides the evaluation of the trustworthiness of data and node. This method also copes with the malicious attack. But the drawback of this method is it doesn't evaluate the capacity of the channel or the channel parameter is not calculated. Channel is an important factor in wireless communication. In this title, we focus on the channel estimation and packet loss is also calculated. It identifies whether the misbehavior is due to channel weakness or some malicious attack.

Khaleel Mershad and Hassan Artail [7] has proposed "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" In this title, we study the security of data messages exchanged between users and RSUs and the location privacy of VANET users who exchange these messages. However, they use asymmetric encryption systems, mainly the elliptic curve cryptography (ECC) standard. We, on the other hand, use asymmetric schemes [Advanced Encryption Standard (AES)] and propose an approach to increase its security to a high extent by using a hierarchical-based encryption function.

Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl [8] have proposed "Graph-Based Metrics for Insider Attack Detection in VANET Multi-hop Data Dissemination Protocols" In this title, we propose three graph-based metrics to gauge the redundancy of dissemination protocols. We apply our metrics to a baseline protocol, a Geo-cast protocol, and an aggregation protocol using extensive simulations. Besides, we point out open issues and applications of the metrics, such as colluding attackers and eviction of attacker nodes based on detected attacks.

Results show that Advanced Adaptive Geo-cast behaves almost optimally from a routing efficiency point of view but fails to offer sufficient redundancy for data consistency mechanisms in many scenarios. The simulated aggregation protocol shows sufficient redundancy to facilitate data consistency checking. In this title, we assess different data consistency approaches for VANETs. Among these, we identify redundancy as a promising approach, particularly for multi-hop protocols. Representing a message transfer of a multi-hop protocol as a directed graph, we derive metrics to assess communication redundancy. In this title, we present extensions of the metrics and perform extensive simulations to show that sufficient data redundancy for consistency checking can be achieved at the cost of higher bandwidth usage and smaller information dissemination areas or reduced information utility.

Kan Zheng, Senior Member, IEEE, Fei Liu, Qiang Zheng, Wei Xiang, Senior Member, IEEE, and Wenbo Wang, Member, IEEE [9] has proposed "A Graph-Based Cooperative Scheduling Scheme for Vehicular Networks" In this title, we propose the use of graph theory to formulate the problem of cooperative communications scheduling in vehicular networks title, we investigate these cooperative relaying problems in cellular-based vehicular networks with V2V communications by proposing a new graph-based approach. Most existing graph-based resource scheduling methods fall under two categories: 1) graph coloring and 2) maximum weighted matching (MWM) in a weighted bipartite graph (BG).

Wen-Hsing Kuo and Shih-Hau Fang [10] has proposed "The Impact of GPS Positioning Errors on the Hop Distance in Vehicular Ad-hoc Networks (VANETs)" In this title, we study the impact of GPS positioning errors on the operation of Vehicular Ad-hoc Networks. To the best of our knowledge, this important issue has not been investigated before. First, we formulate a straight-road model. Then, to reduce the computational complexity of finding the expected degradation, we propose an approximate formula. The results of the simulations show that GPS errors do indeed degrade the hop-distance in VANETs. Moreover, the future approximation method yields good accuracy under sparse density conditions. There are no studies on the impact of GPS errors on the performance of VANETs. Therefore, to address this research gap, we focus on the issue in this title and propose an estimation approach. We conduct simulations and try to identify trends in the results, and also evaluate the accuracy of the future approximation method. We find that positioning errors result in significant degradation of the hop distance, while our approximation method can accurately estimate trends when the traffic density is sparse. Although we only consider the straight road model in this title, we hope that our results will motivate the study of more complicated road topologies, such as cross or grid networks.

III. PROPOSED WORK

Vehicular Ad-hoc communication is a challenging issue due to the different velocity of vehicles and unstructured networks. Nowadays vehicular ad-hoc network play the important role for safety, people time importance, emergency, and congestion avoidance, etc. due to modernization of communication network, its real application are utilized under subordinate vehicular ad-hoc network and provide the accuracy as well as safety to the traveler or passengers. VANET is a semi ad-hoc network because some device is static i.e. roadside unit (RSU) and some of them movable i.e. vehicles, all together form a network and communicate with each other through of them. Communications between the vehicles through RSU or directly vehicle to vehicle if both vehicles are under the range of each other. In the VANET scenario, every vehicle communicates and monitors through RSU. Roadside unit is a centralize unit whose monitor, congestion aware, security provider and accidental case aware on a particular road map that transfers the message to every vehicle whose under the range of RSU. VANET security is important because of the leak of information cerate the hazard to unavoidable problem i.e. accidental arrival, congestion, etc. In the proposed VANET security mechanism roadside unit are monitor all the vehicle and sends control message for communication purpose, while any vehicle capture the another vehicle information and misuse the information, than this type of activity watch through the RSU and send the alert message to the attacker vehicle, so that in future not create any hazard to the communication system. Roadside unit watches the road map traffic, each vehicle speeds and time to time send the alert message if congestion occurs under the road map so that new arrival vehicles before travel-aware about congestion status and wait the ideal time. RSU responsible to manage traffic load, vehicle activity and send alert instruction for vehicle speed control (low, medium, high) if needed. Proposed VANET security system inbuilt in a roadside unit, whose watch the activity of each vehicle and if they found any of them activity abnormal so that RSU eliminate vehicle from the network and trusted network form.

Proposed Algorithm

VANET security algorithm provides trusted and congestion-free vehicular communication, where the

communication between vehicles through the roadside unit. Initially, the road map captured by the RSU and that provides the radio zone to all vehicles so that vehicle to vehicle and vehicle to RSU are communicated and transfer the message to genuine receiver devices. In this algorithm describe the combined approach of different module whose provide secure communication to the VANET.

Algorithm: Secure vehicular communication using Roadside unit (RSU) trust management scheme

Input: V: number of vehicles

RSU: roadside unit
rn: radio range 550 m
sp: speed of vehicle
cn: congestion status (ideal, congested)
a: attack identifies
*T: roadmap area 1100*1100m2*
Output: precision, communication overhead, average delay, throughput.
Procedure:
RSUs (store the T information)
RSUb (broadcast communication message to all V whose in rn)
If V in rn and T is cn == ideal then
V communicate to RSU
V(move under T)
RSU (store information about V in particular T)
RSU (watch the V activity)
V communicate with Vn or RSUn
End if
While RSU monitor T in cn == congested do
RSU sends congestion alert message to V and next RSU
Synchronized the Vn through sp control
Vn send cn information to other Vm
Wait cn ideal condition
End do
If V1 send data to Vn than
If V1 && Vn in rn of RSU then
RSU (forward data to Vn)
Else
Vk (forward data to Vn)
End if
RSU watch the activity of Vk
If RSU detect Vk capture the V1 data and forward! = true then
RSU send warning message to Vk
If Vk ignore warning message then
Vk under a
Eliminate Vk from T
RSU broadcast alert message to all V
V not communicate with Vk
End if
End if
End if

IV. SIMULATION PARAMETERS

In this section describe simulation analysis results through various parameters, for those analyses apply the network simulator-2 and generate network depended analysis etc.

VANET Scenario: In the VANET scenario the four RSU units are in corners where the vehicle is cross is permanent and not changing their location. The function of RSU is to control the whole communication of vehicle-related to the major issues of accidents, congestion, and security. The vehicles are forwarding traffic status to other vehicles for control traffic and other important actions and also the RSU unit is also involved in that communication. The whole work on three protocols Base-line, ART and proposed are simulated in the same VANET scenario.

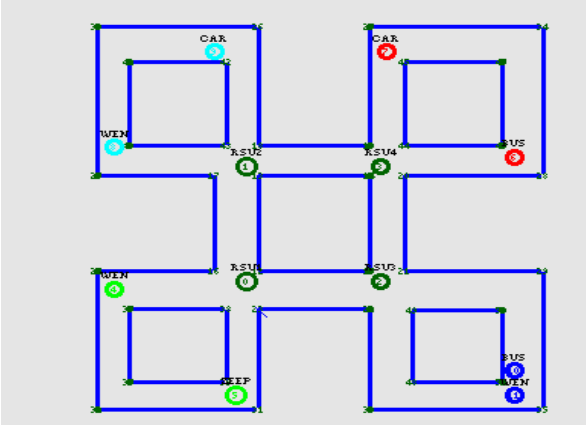

Fig 1: VANET Architecture

Overhead Analysis: In this graph, the flooding analysis Traffic overhead of vehicles is measured and observe that the attacker presence has dropped more packets and due to that data receiving is minimizes. The performance of the base-line and ART is provided better performance but proposed RSU passed communication provides better results and also controls the congestion possibility in network. If in the network due to malicious effect NRL enhanced means delay enhanced. These packets are unwanted. The proposed security scheme against dropping attack is to secure the network performance and providing request packets delivery.

Average end to end Delay Analysis: The number of traffic status packets are drop in network because of attacker misbehavior. The routing protocol existence is also in VANET and the vehicles continuously send and receive traffic data in the network for the better driving facility on roads. In this graph, the delay analysis of the Base-line, ART and the proposed scheme is calculated is given simulation time. The delay in proposed RSU based communication network that means the overhead is

definitely minimized and also the packet receiving is network is enhanced in VANET.

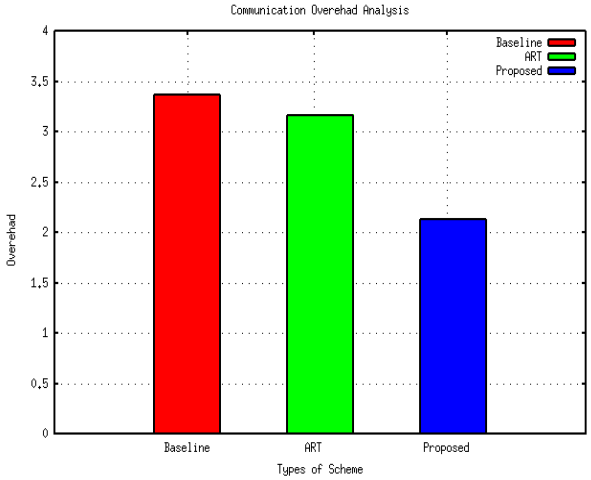

Fig 2: Overhead Analysis

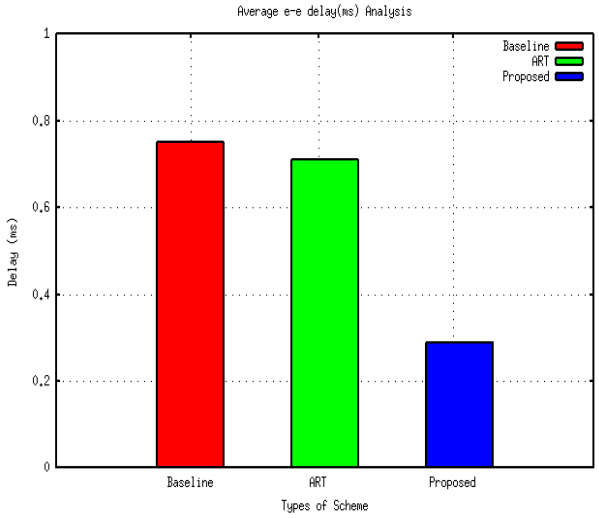

Fig 3: Delay Analysis

Precision Per unit of Time Analysis :- In this graph, the Precision performance of precision-Baseline, Precision-ART and proposed RSU based communication is assessed and observe that the proposed scheme is effective to identify the attacker and recover about more than 90% performance as compared to other performance. The other performance in a network is also better but the proposed scheme provides better results than the other two schemes in a simulation time of 500 seconds This network communication is likely the same as Ad hoc network communication but also easily affected by malicious drives and attackers. The attacker's existence is blocked by RSU for providing secure communication between vehicles.

Throughput Analysis: - Every vehicle is communicated with each other through an established connection for receiving current traffic status. The vehicles are drive on that path according to the traffic information of beginning vehicles. The throughput performance of the proposed security scheme provides better results because the V to RSU based communication is handled the traffic load efficiently in the network as compared to existing Base-line and ART trusted schemes in VANET. The traffic in the proposed scheme is handled properly because of that the possibility of congestion is also reduced.

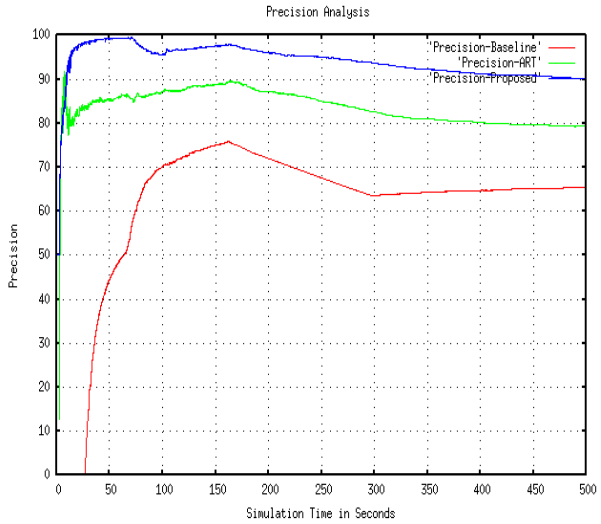

Fig 4: Precision Per unit of Time Analysis

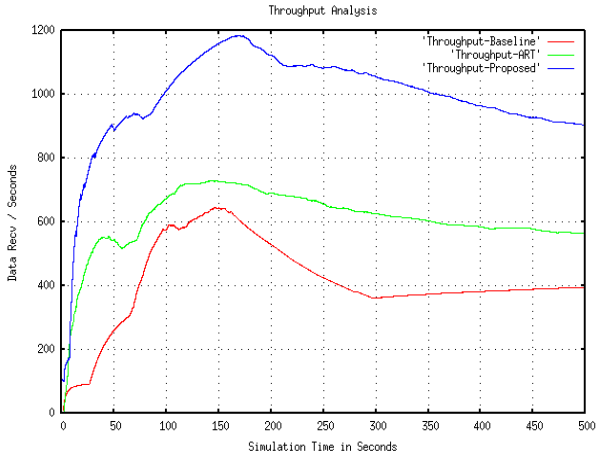

Fig 5: Throughput Analysis

Parameters	Baseline	ART	Proposed-RSU
Data Send	17506	18670	27448
Data Receives	11452	14807	24740
Precision	65.42	79.31	90.13
Communication Overhead	3.37	3.17	2.13
Average Delay	0.75	0.71	0.29
Data Drop	6054	3863	2708

Summarized Performance Analysis:- In this table, we visualized that in Base-line and communication overhead is more for securing V to V performance. The Normal Routing Load (Traffic request packets by Traffic data

received) is enhanced and also the end to end delay is enhanced in the network. The reliable RSU units provide the secure V to V communication (V to RSU Communication) and network performance is better than the rest of the two vehicular security schemes.

V.CONCLUSION AND FUTURE WORK

The self-organized network provides better communication and coordination between the vehicles through established Vehicle to Vehicle (V to V) and Vehicle to Road Side Unit (V to RSU) communication in network. The previous work is a discussion that provides the novel idea of simulation proposed security algorithm. In this research, we proposed a new secure Hole Attack Prevention (HAP) algorithm to detect the malicious vehicles and disabled their communication capabilities for further communication in the network. The three scenarios are proposed in this research. The first scenario of the road network is based on V to V Base-line communication. Second is the ART security scenario and here it is observed that the network performance is better in the presence of an attacker. But in both the scenario the attacker presence is not completely blocked by any other vehicle. In the third proposed, RSU based communication scheme is not only detected but also prevent attackers. The main advantage of applying security in V to RSU is that, if the attacker is detected then their particular information is easily broadcast to all the RSUs for alert in future from that malicious vehicle. After all, this information is broadcasting after block the malicious vehicle/s. The proposed security scheme provides zero attacker infection and minimized packet dropping of traffic packets. The minimization in delay represents the better vehicle movement. The proposed RHA is recovering about 97 % performance as compare to the normal VANET scenario. The security criteria are not resolved from this particular research. In VANET network road accidents and road construction information issues are also affected the network performance, the malicious driver is the main obstacle for forwarding the important message to another driver. In the future, we proposed mobility-based communication with RSU. In this scheme try to provide a clear path for high-speed vehicles and identified the vehicle that modified or not follow that policy of vehicle communication.

REFERENCES

[1]. Sudha Dwivedi, Rajni Dubey, Nirupama Tiwari "Trust-Based Scenario using AES Encryption in VANET" IJARCSSE Volume 6, Issue 8, August 2016.

[2]. Wenjia Li, Member, IEEE, and Houbing Song, Senior Member, IEEE "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks" IEEE transactions on Intelligent Transportation Systems, Vol. 17, No. 4, April 2016.

[3]. Gaikwad Priti G., Nilam Patil "Survey on Vehicular Ad Hoc Networks Security" DOI: 10.15680/IJIRCCE.2017. Vol. 5, Issue 1, January 2017.

[4]. Ayana Santhosh, Bini babu, Jain maria, Ashly Angel "Secured Data Transmission Method for Van Networks" Secured Data Transmission Method for Van Networks (IJSTE/ Volume 2 / Issue 10 / 026 April 2016

[5]. Divya A C, K Vyshnavi, Kusuma N, Revathy S "Increasing Trustworthiness In Data Transfer Of Vehicular Ad Hoc Networks" IJARIIE Vol-2 Issue-5 2017 -ISSN(O)-2395-4396 C-1608.

[6]. Arya Chandran B S & Ajay V G "VANET Based Communication Scheme in Network Environment" Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-5, 2017.

[7]. Khaleel Mershad And Hassan Artail "a framework for secure and efficient data acquisition in vehicular ad hoc networks" IEEE transactions on vehicular technology, vol. 62, no. 2, February 2013.

[8]. Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl "Graph-Based Metrics for Insider Attack Detection In Vanet Multi-hop Data Dissemination Protocols" IEEE Transactions On Vehicular Technology, Vol. 62, No. 4, May 2013.

[9]. Kan Zheng, Senior Member, IEEE, Fei Liu, Qiang Zheng, Wei Xiang, Senior Member, IEEE, And Wenbo Wang, "A Graph-Based Cooperative Scheduling Scheme For Vehicular Networks" IEEE Transactions On Vehicular Technology, Vol. 62, No. 4, May 2013.

[10]. Wen-Hsing Kuo and Shih-Hau Fang, "The Impact of GPS Positioning Errors on the Hop Distance in Vehicular Ad-hoc Networks (VANETs)" International Conference on Computing, Networking and Communications (ICNC) Workshop on Computing, Networking and Communications 2013.

[11]. Maurice J. Khabbaz, Hamed M. K. Alazemi, and Chadi M. Assi "Delay-Aware Data Delivery in Vehicular Intermittently Connected Networks" IEEE transactions on communications, vol. 61, no. 3 march 2013.