IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Invention and Implementation of NTBS Clustering Protocol for VANET

Venkatamangarao Nampally[1*], M. Raghavender Sharma[2]

[1]Department of Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, India
[2] Vice-Principal, University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India

[*]*Corresponding Author: n.venkat013@gmail.com, Mob. 8897393431*

Available online at: www.ijcseonline.org

18/May/2018, Published: 31/May/2018

***Abstract*—** Vehicular Ad hoc Networks (VANETs) are the promising approach to provide traffic, safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. Communication is not for only reliable data delivery but also the achieving the reliability. In this paper, we present how to obtain best communication in VANET system by using Transitive Trust Relationships concept and thus improving the performance of the authentication procedure of the whole network in a cluster. Proposed NTBS protocol not only adapts the concept of Transitive Trust Relationships but also improves the performance of the authentication procedure and it provides best communication with good security. We implement NTBS protocol in NS2 Simulator. NS2 is open source and discrete event-driven, object-oriented and freely available simulation tool to simulate and analyze dynamic nature of communication networks. It is also a powerful tool to develop new protocols and functions. It provides support for OSI and TCP/IP protocols stack and many standard routing and application protocols for wire and wireless networks. NAM is used to display the process of simulation.

***Keywords*—** VANET, TTR, NS2, NAM, TCL, NTBS, OBU, RSU, AS, Clustering Protocol.

I. INTRODUCTION

An Ad Hoc Network is self configuring network in which mobile routers forming arbitrary topology with peer to peer connection. It is decentralised type of wireless network [1]. There are two types of networks available in ad hoc network MANET and VANET. VANETs are likely to become the most relevant realization of MANET. VANET is a type of ad hoc network in which vehicles act as nodes. In VANET system, VANET is a term used to describe the spontaneous Ad Hoc Network formed over vehicles moving on the roadside. VANET could be differentiated from MANET by the movements of the nodes. Another differentiating parameter between MANET and VANET is speed of the nodes. Normally speed of the nodes in MANET is very slow comparing to the nodes of VANET. Inside a VANET, nodes can communicate with another node either directly or indirectly using the existing infrastructure [2]. It consists of number of reliable sensors within it for communication. Each vehicle in this network contains a device which is used for sending and receiving data. VANET aims to insure safe drive by improving the traffic flow and therefore significantly reducing the car accidents. The primary goal of VANET is to provide road safety conditions to drivers as well as passengers in emergency situations. VANET is an emergent technology with promising features as well as great challenges especially in communication. All vehicles are moving freely on road network and communicating with each other or with RSUs and specific authorities. In VANET, vehicles are connected not only to form a wireless network but also to share information. Here, cars will communicate with one another to drive cooperatively in order to avoid collisions and improving efficiency. It is difficult to maintain routing path among vehicles because in VANET system the network topology is dynamic topology and the wireless communication links are inherently unstable. So, there will be frequent disconnect of network. DSRC is a short range communication system for safety and infotainment applications in both V2V and V2I environment.

A. Domains and components of VANET system

Actually the development of VANET system architecture varies from region to region. Generally, domains which are available in VANET system are: the vehicle domain, the mobile device domain, and an infrastructure domain [3]. The vehicle domain comprises all kinds of vehicles such as cars and buses. Using the on-board unit i.e. node, vehicles can communicate among themselves and with roadside units. The mobile device domain comprises all kinds of portable devices like personal navigation devices and smart phones. infrastructure domain contains all types of infrastructure used

in VANET system. Infrastructure domain further contains two domains within it are:

- **The Roadside Infrastructure Domain:** In the roadside infrastructure domain, there are roadside unit entities like traffic lights.
- **Central infrastructure domain:** The central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers (VMCs).

But, CAR-to-CAR Communication Consortium (C2C-CC) comprises domains namely: in-vehicle, ad hoc and infrastructure domain [4].

The architecture of a VANET compromises the wireless on-board unit (OBU), the Roadside unit (RSU), the authentication server (AS), and CA. VANET system compromises the essential components: OBU (On Board Unit), RSU (Road Side Unit) and AS (Authentication server). Road side units (RSUs) and On-Board units (OBUs). RSUs are widespread on the road edges to fulfill specific services.

- **OBU:** By using the on-board unit, vehicles can communicate among themselves and with roadside units. OBUs are installed in vehicles to provide wireless communication capability and each vehicle's OBU is equipped with security hardware (e.g., trusted platform module), including an Event Data Recorder (EDR), and a Tamper-Proof Device (TPD) so that an attacker cannot obtain information about the vehicle from the OBU. The EDR is responsible for recording important data about the vehicle, such as the location, preload common key, and access log. The TPD provides the cryptographic processing capabilities.
- **RSU:** RSUs are deployed on intersections as an infrastructure to provide information or access to the internet for vehicles within their radio coverage and acts as mediator between AS and OBU. RSU can be connected with another one in two ways: wired and wireless.
- **AS:** The AS is responsible for installing the secure, fast parameters in the OBU to authenticate the user.
- **CA:** Centralized authority which registers the vehicles before they are allowed to operate on the road.

B. VANET Communication Patterns Types

Based on IEEE 802.11p, the Dedicated Short Range Communication system supports two types of communication environments:

- Vehicle-to-Infrastructure (V2I) and
- Vehicle-to-Vehicle (V2V) communication
- Cluster based communication model (V2C)
- Vehicle-to-Broadband

1) Vehicle to Infrastructure (V2I) Communication

If communication exists among infrastructure (RSU) and vehicles then the communication is called as vehicle to infrastructure communication i.e., among RSU and vehicles communication. This is also called as V2I communication. The fundamental architecture of this communication model is fixing the antenna (Road Side Unit) at the side of the road and the signal is propagated from it. Each vehicle will get the signal to communicate with other vehicle from either the nearby Road Side Unit (RSU) or OBU. Identity of each vehicle will be available at the RSU. All the RSUs will act as the router in vehicular ad hoc network communication scenario.

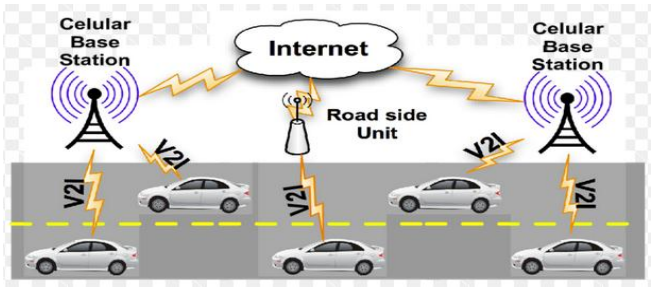

Figure 1. V2I communication

2) Vehicle to Vehicle V2V Communication

In this (V2V) Communication architecture each vehicle is manufactured with On Board Unit (OBU), which is capable of sending and receiving the messages among vehicles. If communication is done among Vehicles then that communication model is called Vehicle to Vehicle communication. Each node in V2V model functions as the router to transmit/receive the messages. Achieving the authentication mechanism in V2V is crucial than V2I authentication mechanism. There exists no centralized authority to perform the authentication procedures of vehicles.

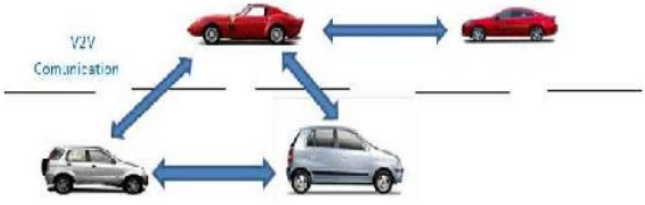

Figure 2. V2V Communication

3) Cluster Based Communication Model

A group of VANET nodes within a radio range can form a cluster environment. In other words a cluster is a group of nodes that communicate with each other without disconnection. Formation of vehicle groups into clusters is significance in VANET system. Clustering is a mechanism of grouping vehicles into clusters. A good clustering

algorithm for VANET system should not only stable but also has lower cluster maintenance overhead by emphasizing creation of excellent clusters. In VANET system, vehicles that are willing to share information will be grouped into clusters. In VANET system clustering is used to improve routing scalability and reliability. Clustering is a mechanism of grouping of vehicles based upon some predefined metrics such as density, velocity, and geographical locations of the vehicles to delivery of the efficient data in VANETs. Every node in the cluster structure plays one of three roles: Cluster Head (CH), Cluster Gateway (CG), and Cluster Member (CM). While creating a cluster, it should be ensure that the CG of any cluster is not frequently crossing the cluster boundary. After considering the drawbacks of the previous communication models in vehicular ad hoc network, researcher proposed novel communication architecture knows as Cluster Based Communication Model. All the vehicles are grouped into various numbers of clusters depending on the density of the vehicles. One vehicle is chosen as the cluster head for each cluster by considering the various parameters. Cluster head will act as the server and all the nodes under a cluster head will act as the clients. All the cluster heads are interconnected in such a way that it would be easy to disseminate the messages to other cluster heads. Cluster head will store all the acquired data in its database and it will distribute the data to its clients as it is requested by the nodes.

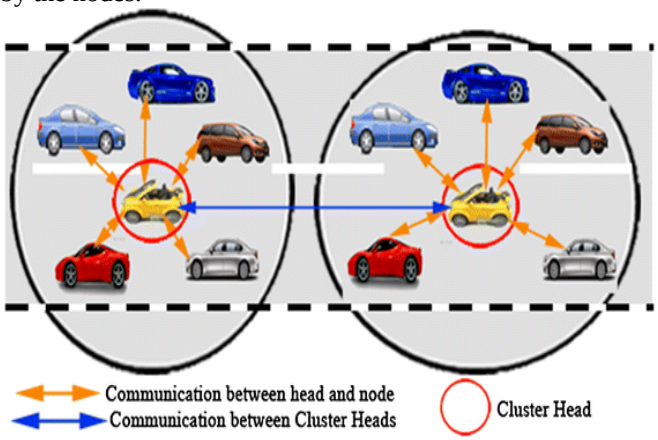

Figure 3. Cluster based communication model

4) Vehicle-to-Broadband Communication

In this communication model, vehicles can communicate via wireless broadband mechanism such as 3G/4G. This type of communication will be useful for active driver assistance and vehicle tracking.

C. Characteristics of VANET system

VANET system is different in characteristics from MANET. The main characteristics of VANET system are: [5].

- High Mobility
- Rapidly changing network topology
- Unbounded network size
- Frequent exchange of information
- Wireless Communication
- Sufficient Energy
- Better Physical Protection

D. Applications of VANET system

Depending on the type of communication either V2I or V2V, we are arranging the applications of VANETs into the following classes:

- Safety oriented,
- Commercial oriented,
- Convenience applications and
- Productive applications

1) Safety oriented: The Road safety applications can be classified as:

- **Real-time traffic**: This can play an important role in solving the problems such as traffic jams, avoid congestions and in emergency alerts such as accidents etc.
- **Co-operative Message Transfer:** Slow/Stopped Vehicle will exchange messages and co-operate to help other vehicles.
- **Accident Notification:** A node involved in an accident would broadcast warning messages about its position to other nodes.
- **Cooperative Collision Warning:** Alerts drivers potentially under crash route.
- **Traffic Vigilance:** The cameras can be installed at the RSU that can work as input and act as the latest tool in low or zero tolerance campaign against driving offences.

2) Commercial oriented: These provide the driver with the entertainment and services as web access, streaming audio and video. The Commercial applications can be classified as:

- **Remote Vehicle Personalization/ Diagnostics:** Helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to an infrastructure.
- **Access of Internet:** in VANET system Vehicles can access internet through RSU if RSU is working as a router.
- **Value-added advertisement:** This is especially for the service providers, who want to attract customers to their stores. This application can be available even in the absence of the Internet.

3) Convenience applications: These applications mainly deal in traffic management. The Convenience applications can be classified as:

- **Route Diversions:** Route and trip planning can be made in case of road congestions.
- **Electronic Toll Collection:** Payment of the toll can be done electronically through a Toll Collection Point as shown in Figure. A Toll collection Point shall be able to read the OBU of the vehicle.
- **Active Prediction:** it anticipates the upcoming topography of the road.

4) Productive applications: We are intentionally calling it productive as this application is additional with the above mentioned applications. The Productive applications can be classified as:

- **Time Utilization:** A traveler can transform jam traffic into a productive task and read on-board system and read it himself if traffic stuck. One can browse the Internet when someone is waiting in car for a relative or friend.
- **Fuel Saving:** toll fee collection can be paid without stopping vehicle. Thus, saving of fuel around 3% when we compare to normal situation.

E. Security Requirements in VANET

Security is a state of being or feeling protected from harm or attack. Security Requirements for VANETs are:

- **Authentication :** An authentication framework is necessary to enable receivers of broadcast data to verify that the received data really originates from the claimed node without modification. Authentication methods categorized into two groups: message authentication and entity authentication.
- **Integrity:** Integrity is required between two communicating nodes to protect data accuracy, which is main security issue desirable in VANETs. Information should not be altered without detection.
- **Access of Internet:** in VANET system Vehicles can access internet through RSU if RSU is working as a router.
- **Location-verification:** This is necessary to prevent many attacks and is helpful in data validation process.
- **Nonrepudiation:** Nonrepudiation prevents either sender or receiver from denying a transmitted message.
- **Privacy:** The protection of personal information of drivers within the network from other nodes but extracted by authorities in case of accidents is a major privacy issue which is desirable for VANETs.
- **Key-Management:** The key is used to encrypt and decrypt information during communication process. When designing security protocols for networks like VANET, the issue of key management must be resolved.
- **Pseudonymity:** Pseudonymity is the state of describing a disguised identity. A holder that is one or more human beings is identified but do not disclose their true names.
- **Confidentiality:** The challenge to protect data content from the adversaries is confidentiality. It assures that private or confidential information is not made available.

The remainder of this paper is organized into as follows:
Section II contains a review of related work. Section III explains methods which are used in VANET secure communication, section IV gives proposed work. In Section V, we give the analysis and simulation results. At last we give conclusion, acknowledgments', and references are given which are used for preparing this paper.

II. RELATED WORK

In this section we review previous research works in the field of VANET system by using clustering protocols. For the review, we have discussed the taxonomy of clustering approaches and grouping them into six groups and review these protocols. It has been demonstrated that problem of VANET is vehicle protection from theft, prevention from sudden accidents, unwanted malicious attacks. In this regard, communication with other vehicles is final solution. So, in order to dissemination of messages from one vehicle to other vehicle, communication is must. Many schemes emerged to achieve communication among nodes.
Gerlach [6] describes the security concepts for vehicular networks. Maxim Raya and Jean-pierre Hubaux [7] preloaded each vehicle with a large number of anonymous public and private key pairs. However, this approach works good but with high computation cost, high storage space, and high communication overhead. And also, this scheme is not suitable for very highly dynamic environments. Hubaux et al. [8] has taken a different perspective of VANET security and focused on privacy and secure positioning issues. They point the importance of the trade-off between liability and anonymity and also introduce Electronic License Plates (ELP) that is unique electronic identities for vehicles. El Zarki et al. [9] described an infrastructure for VANETs and briefly mention some related security issues and possible solutions. Very related to VANET security is the security of the electronic systems in a vehicle that are actually responsible for transporting or generating the data before it is sent. Zhang [10] proposed a RSU-based message authentication scheme, which uses the symmetric key hash message authentication code, instead of a PKI-based message signature, in order to reduce the signature cost which results in low storage space. However, this method also leads to a high computation cost. Gowtham [11] achieved communication between nodes take place in secured way by using security algorithms similar to ECDSA and TESLA. VANET uses a hardware known as TPD to provide security to nodes in communication process. In 2010, J.T. Isaac, S. Zeadally, and J.S. Camara published a paper on "Security attacks and solutions for vehicular ad hoc networks" [12].

To achieve fast communication with security is one of the major problems in VANET. From these, ECC [13] method by Menezes, S. Vnstone, and D. Hankerson achieved best security but with high computation cost. So, in order to overcome this disadvantage, Sirwan A Mohammad and Dr. Sattar [14] developed wireless network based on ns2. But, unfortunately, this scheme also leads to high storage space and also to achieve general authentication in this scheme, requires many steps. But, these schemes lead to long authentication latency. Clustering has been widely used to route the message to their final destination. Wang et al. [15] proposed another position based clustering algorithm. It explains a cross layer algorithm based on hierarchical and geographical data collection and dissemination mechanism. Fan et al. [16] proposed a clustering scheme called where a utility based cluster formation technique is used by extending the definition of spatial dependency. All the neighbouring vehicles periodically send a status message. After receiving this message, each vehicle chooses its CH based on the results produced by the utility function. The node with the highest value is chosen as the CH. Wolny [17] optimized the existing DMAC algorithm so that road traffic mobility is represented in an efficient manner. Farhan et al. [18] proposed an algorithm for improving the accuracy of GPS devices called Location Improvement with Cluster Analysis (LICA).Blum et al. [19] used a PKI with virtual infrastructure where a set of elected CHs are responsible for disseminating messages after digitally signing them. This scheme is intended only for the attack called intelligent collisions. Sivagurunathan et al. [20] proposed a self-organized key management system based on clustering. In this model, the network is divided into number of clusters based on the concept that any user can sign any other public key. Cheng et al. [21] proposed an innovative car society clustered network based on an imaginative classification scheme. Almalag et al. [22] proposed a clustering mechanism in which clustering is done on the basis of similarity in vehicles. Souza et al. [23] proposed a clustering technique that uses the Aggregate Local Mobility (ALM) metric for initiating cluster re-organization. Rawshdel et al. [24] proposed a clustering technique in which vehicles showing similar mobility pattern are grouped in same cluster. Shea et al. [25] proposed a clustering technique in which nodes use the Affinity Propagation (AP) method to send message to one another. Kayis et al. [26] proposed a clustering technique in which vehicles are classified into groups based on speed range. The author defined seven groups of speed that a vehicle can use and the vehicle falling in same group belonging to same cluster. Fan et al. [27] proposed a lane-based clustering algorithm based on the traffic flow of vehicles. Zhenxia Zhang et al. [28] proposed a novel k-hop clustering approach. This system improves network stability and reduces the overhead and the latency caused by rote path recovery. Merij [29] proposed the use of a cryptographic based categorization that is easy and plain to understand since the similar approach it takes as done in traditional network security solutions. Sun [30] proposed an identity-based security system for VANET that can effectively solve the conflicts between privacy and tractability. The system uses a pseudonym-based scheme to preserve user privacy. Azogu [31] proposed an Asymmetric Profit-Loss Markov (APLM) model that measures the integrity level of the security schemes for VANET content delivery. Tim Leinmuller in 2006 [32] aimed to define a consistent & future-proof solution to the problem of V2V/V2I security by focusing on SEVECOM (Secure Vehicle Communication). Zuowen in 2010 [33] proposed an improved privacy-preserving mutual authentication protocol for vehicle ad hoc networks by using secure identity-based group blind signature, the private encryption system and the public encryption system.

III. METHODOLOGY

A. Clustering Method

A cluster is a group of nodes that communicate with each other without disconnection. Formation of vehicle groups into clusters is significance in VANET system. Clustering is a mechanism of grouping vehicles into clusters. A good clustering algorithm for VANET system should not only stable but also has lower cluster maintenance overhead by emphasizing creation of excellent clusters. In clustering of VANET system each cluster has cluster member (CM), cluster head (CH), and cluster gateway. A cluster member is responsible for coordinating other cluster members who are inside that cluster. A cluster head is responsible for coordinating all cluster members and is responsible for gathering data from any node of cluster sends that data to another cluster head. And it is also responsible for gathering of traffic status information. A cluster gateway is a node in a cluster is responsible for communicating nodes which are belonging to different clusters. The goal of clustering in VANET system is to establishment of a certain structure among vehicles before information transferring. Clustering increases the delivery rate. In cluster-based topology control, an implementation of linked cluster architecture must achieve the following tasks. Clustering is a process combination of three processes as:

- **Cluster formation:** it is the process of making a cluster by using cluster formation algorithm.
- **Cluster maintenance:** it is the process of managing a cluster. and
- **Cluster reorganization:** it is the process of either making new clusters or splitting or merging existing clusters.

B. Data Collection in a Cluster

In a cluster each CH on a CS must collect data from all active vehicles members and inform them of retransmission

if it is deemed necessary. To do this, each elected CH executes various iterations. During the first iteration the reservation of time slots is static, i.e. the CH assigns a time slot to each block of its CS. So, the CH generates a Token packet and sends it to the first block of its CS. Then, it waits to receive a Data packet for a sixth time slot. If it does not receive data during this time, it regenerates a new Token, it sends it to the next block, so on until the last block of the CS. Along with this, it reserves both tables RSV and Ack. based on the Data packets received from MVs. Furthermore, the New Arrivals from vehicles (NA) are allowed fixed number of slots equal to the number of lanes.

C. *Clustering Protocols Taxonomy*

The taxonomy of clustering protocols in VANET system is:

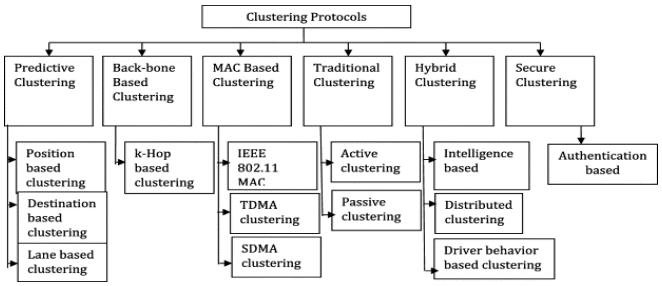

Figure 4. Taxonomy of clustering in VANET system

D. *Transitive Trust Relationships*

In a VANET system, an LE authenticates nearby vehicle into a trustful vehicle. As the number of LEs is finite, an LE is not always near to the OBU. Even if the user is well meaning, the Vehicle must still wait for the nearest LE and then perform the authentication procedure. Hence, there is a need for an efficient and a reliable communication mechanism. To overcome this problem, we follow transitive trust relationships and we propose a key exchange protocol to improve the performance of the authentication procedure in V2V communication networks. The protocol is based on the concept of transitive trust relationships, as illustrated in Fig. Let us suppose that initially, there are three vehicles in a VANET system. A trustful vehicle (LE) and two other MVs carrying OBUs. If a vehicle is always capable to give authentication to nearby vehicle then it is called as trustful vehicle, further a vehicle which is not capable to give authentication then it is termed as mistrustful vehicle.

Step 1) the state of the first mistrustful OBU becomes trustful and obtains the sufficient authorized authenticated parameter to authenticate the other mistrustful OBUs when it authenticated successfully with a LE.

Step 2) then this OBU gives authentication to nearby vehicle and makes it into trustful vehicle i.e. temporary LE.

Step 3) then that turning OBU can make change the mistrustful vehicle into trustful.

In V2V communication networks, as the number of LEs is finite, an LE is not always in the Vicinity of the OBU. Even if the user is well meaning, the Vehicle must still wait for the nearest LE and then perform the authentication procedure. Hence, there is an urgent need for an efficient authentication scheme. Here, we propose a key exchange protocol to improve the performance of the authentication procedure in V2V communication networks. The protocol is based on the concept of transitive trust relationships, as illustrated in Fig. Let us suppose that there are three vehicles: A trustful vehicle (LE) and two other MVs carrying OBUs (OBU_i and OBU_j). The state of the first mistrustful OBU (i.e., OBU_i) becomes trustful and obtains the sufficient authorized parameter to authorize other mistrustful OBUs when it is authenticated successfully.

IV. PROPOSED SYSTEM

A. *NTBS Clustering Protocol*

In order to achieve general authentication and to make it secure communication among nodes in a cluster of VANET system, we have proposed Number Theory Based Security (NTBS) clustering protocol method. It gives not only communication but also secure communication. Before a vehicle can join a VANET, its OBU must be authenticated by an LE. When a vehicle wants to access the service or wants to give the service, then it has to perform the login key exchange procedure. If the authentication procedure done successfully, the vehicle is trustful vehicle (TV), otherwise it is considered as mistrustful vehicle (MV).The MV needs an authentication procedure in order to change its state from MV into TV. Thereafter, the trustful vehicles change the MVs into TVs performing the authentication procedure by using Transitive Trust Relationships (TTR). In the same way all vehicles in a cluster get to be authenticated. The state of the LE does not change because the LE is always trustful.

B. NTBS Clustering Protocol Phases

The proposed scheme involves with following procedures:

Table1 Proposed system procedures

Table 1: NTBS key Exchange Protocol Phases

1.LE Registration,
2. NTBS clustering Protocol key generation.
3. Node Authentication

1) LE Registration

(Before initial registration we need LE registration)

LE Registration: First, the LE performs the LE registration procedure with the AS through the manufacturer or a secure channel when it is manufactured. The AS computes the secure key set {PSKi, i = 1, . . . , n} based on the hash-chain method (e.g.,$h2(x) = h(h(x))$) and sends this key set to the LE

and it is stored in the security hardware. An LE can check every vehicle whether that vehicle is trustful or mistrustful.

2) NTBS Clustering Protocol Key Generation

This protocol method allows users so that they can share information by communicating in a smooth fashion with each other by using a key. Here secure communication will exist in network by exchanging secure keys of nodes.

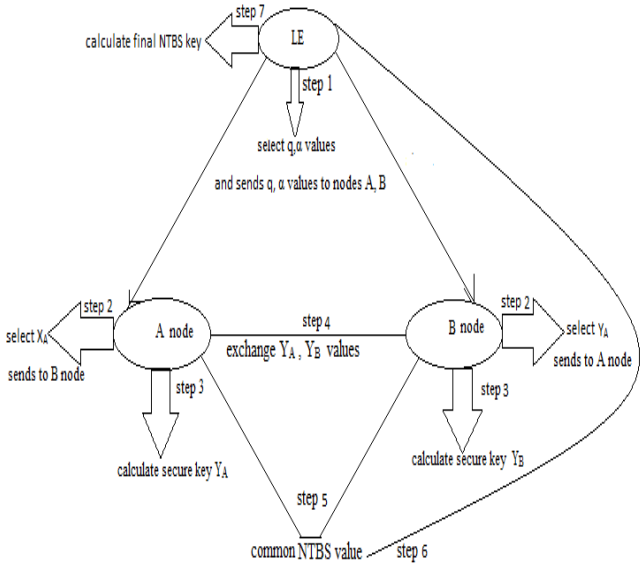

Figure 5. steps in NTBS operation

If we see operations NTBS in table form then next table shows steps occurred inside NTBS clustering protocol.

Table 2: NTBS key Exchange protocol Steps

1.Select a number 'q' such that q ≥ 1 nibble and also Select a number 'α' such that α ≥ 1 nibble	
2. node A chooses a key 'X_A'' such that $X_A \geq$ 1nibble node B chooses a key ' X_B' such that $X_B \geq$ 1nibble and exchange X_A , X_B values	
3. Calculating secure Keys Y_A and Y_B and sends to LE	
By node A	By node B
$Y_A=(((q.\alpha)*x_B)*\text{mod}(q, \alpha))$	$Y_B=(((q.\alpha)*x_A)*\text{mod}(q, \alpha))$
4. Exchange Y_A , Y_B values and	
5. Calculating of common NTBS keys	
By node A	By node B
$NTBS_A=$ $((Y_A)(X_B)\ (Y_B)(X_A)))*\text{mod}(q, \alpha))$	$NTBS_B=$ $((Y_B)(X_A)\ (Y_A)(X_B)))*\text{mod}(q, \alpha))$
6. transfer of common NTBS key to LE	
7. LE calculates $NTBS_{final}$ as : $(NTBS_A*Y_B)\ (NTBS_B*Y_A)$ mod $(NTBS_A + NTBS_B)$	

C. NTBS clustering Protocol Steps explanation

- **Step 1)** In order to communicate with each node to other in a cluster, First LE selects one number 'q' such that q ≥ 1 nibble and another number 'α' that α ≥ 1 nibble. Then LE sends that both q, α values to two nodes which are near to LE.
- **Step 2)** Now that two nodes select normal values 'X_A' (normal key) and 'X_B' (normal key) respectively. Then nodes exchange x_A and x_B values between them.
- **Step 3)** And compute their Secure keys Y_A, Y_B as $Y_A=(((q.\alpha)*x_B)*\text{mod}(q, \alpha))$ and $Y_B=(((q.\alpha)*x_A)*\text{mod}(q, \alpha))$
- **Steps 4)** then they again exchange secure keys.
- **Step 5)** and both nodes compute common NTBS keys as:
  $NTBS_A = ((Y_A)\ (X_B)*(Y_B)(X_A)*\text{mod}(q, \alpha))$ and
  $NTBS_B = ((Y_B)\ (X_A)*(Y_A)(X_B)*\text{mod}(q, \alpha))$
- **Step 6)** that common NTBS values transfer to LE.
- **Step 7)** then LE computes **Final NTBS key** as:
  $NTBS_{final} = (NTBS_A*NTBS_B)\ \text{mod}\ (NTBS_A+NTBS_B)$

This final NTBS key sends to all nodes which are inside a cluster by using transitive trust relationships. Then every node before giving authentication checks whether that being authenticated node having same value equals to $NTBS_{final}$ value or not. If that value is equal to $NTBS_{final}$ then that node will be authenticated. Similarily by using TTR concept communication will be flown in total cluster.

It gives secure communication because it involves with number theory operations. The steps which are inside the NTBS key exchange protocol summarized in below table.

3. Node Authentication Process

Inside VANET system a node can be authenticated either nearby vehicle or RSU or LE. An LE always trustful i.e., it can authenticate nearby vehicles always. But it not possible to LE that always in the suroundings of all vehicles. It stands near to some vehicles only. So, in order to authenticate all vehicles which are inside a cluster, we use TTR concept. This node authentication phase follows following steps.

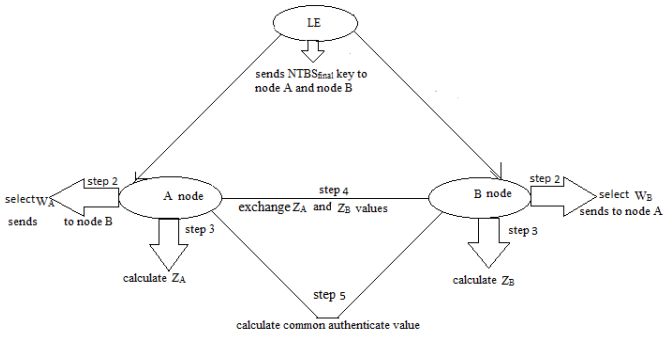

Figure 6. Node turns into TV

Step 1) LE sends $NTBS_{final}$ key to node A and node B respectively.

Step 2) Node A assumes one number W_A such that $W_A \geq 1$ nibble and sends these number to node B, similarly node B assumes one number W_B such that $W_B \geq 1$ nibble. Both nodes exchange W_A ,W_B keys.

Step 3) they calculate Z_A , Z_B values as:

$Z_A = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$

$Z_B = (NTBS_{final} * W_B)\ (NTBS_{final} * W_A)$

Step 4) exchange these Z_A , Z_B values between A,B nodes.

Step 5) and calculate $NTBS_{auth}$ values as:

$NTBS_{auth.A} = (Z_A.NTBS_{final})(Z_B.NTBS_{final})(W_A.W_B.NTBS_{final})$

$NTBS_{auth.B} = (Z_B.NTBS_{final})(Z_A.NTBS_{final})(W_A.W_B.NTBS_{final})$

By using number theory, we can prove

$NTBS_{auth.A} = (Z_A.NTBS_{final})(Z_B.NTBS_{final})(W_A.W_B.NTBS_{final})$

$= (Z_B.NTBS_{final})(Z_A.NTBS_{final})(W_A.W_B.NTBS_{final})$

$= NTBS_{auth.B}$

Both nodes can give same value under multiplication operation in number theory. So, communication will be flow securely among nodes in a cluster.

V. SIMULATION RESULTS

A. *Transitive Trust Relationships concept in NAM*

Transitive Trust Relationships are very important tasks in VANET. In TTR, LE can authenticate any type OBU then that OBU turns into temporary LE (Trustful Vehicle) and authenticate another OBU then that OBU also turns into TV so on. Like this way all vehicles can communicate one with another forming Global VANET.

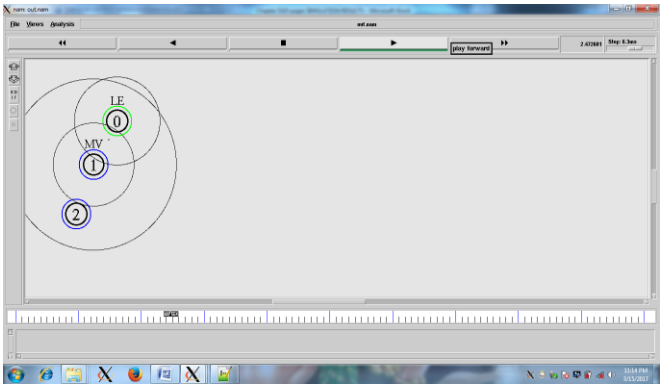

Figure 7. Node changes its form to MV

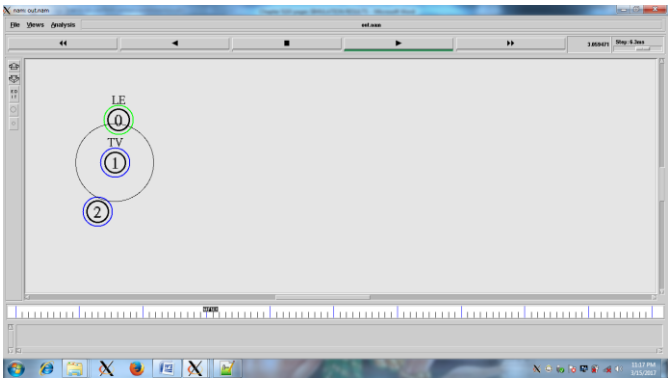

Figure 8. Node turns into TV

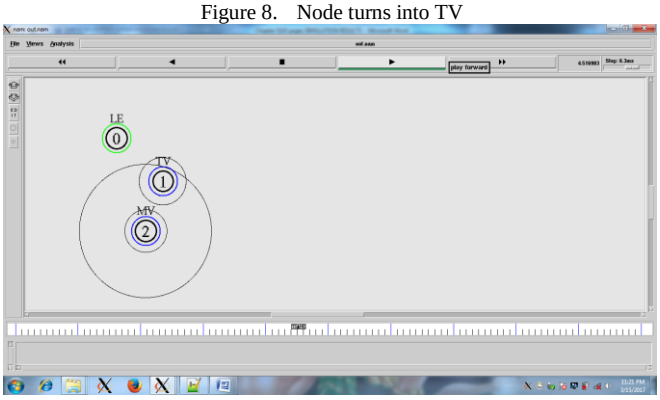

Figure 9. Another node turns into MV

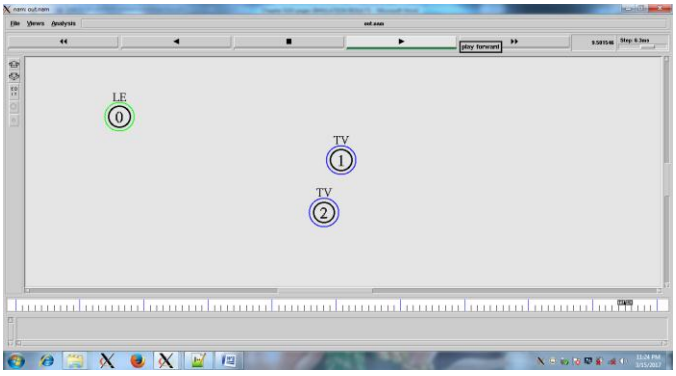

Figure 10. Both nodes turns into TV

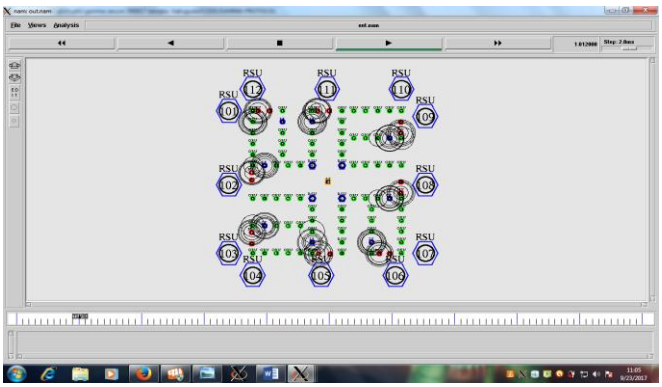

Figure 11. Communication process in a cluster of VANET system

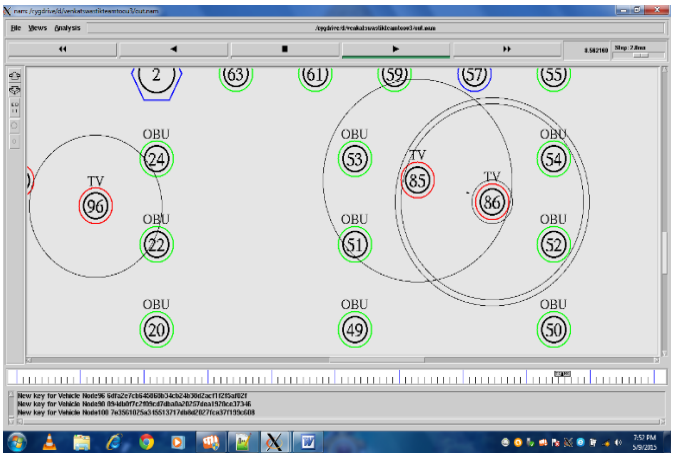

Figure 12. Nodes turn into TV in a cluster

B. *Analysis of NTBS Clustering Protocol*

Following table describes used parameters in order to simulate these model based on TTRs in NS2 simulator.

Table 2: Simulation parameters

Parameters	Values
Network Size	4000m x 4000m
Number of Vehicle Nodes	112
Packet_ Size	1000bytes
Simulation Time	10 sec.
MAC protocol	IEEE 802_11
Number of Authentication Servers	1
Number of LEs	16
Number of OBUs	86

1. Throughput Graph

It is defined as rate of successful message delivery over a channel or aggregate number of packets delivered over the simulation time. Mathematically it can be written as:

Throughput=N/100

Where N is the number of bits bought by all destinations.

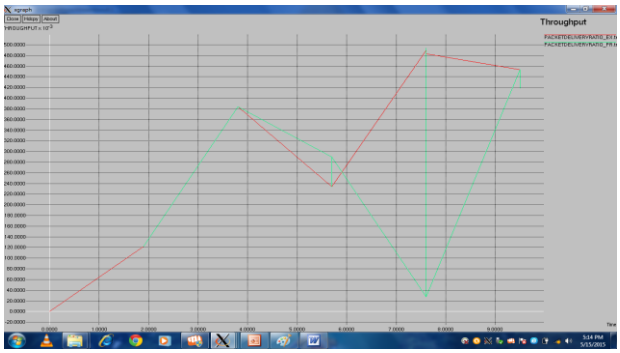

Figure 13. Throughput graph

2. Packet Delivery Ratio Graph

Packet delivery ratio is the ratio of the number of packet received by the destination to the number of packet sent by the sender.

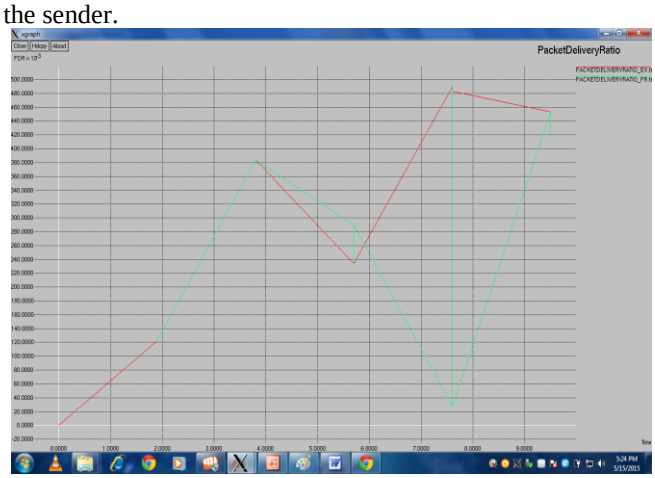

Figure 14. Packet delivery ratio graph

3. Packet Loss Graph

It is defined as number of failed packets to reach destination from source during transmission. Packet loss occurs due to network congestion. Mathematically it can be calculated as:

Packet Loss= N/S

Where N is number of loss packets and S is the number of received packets.

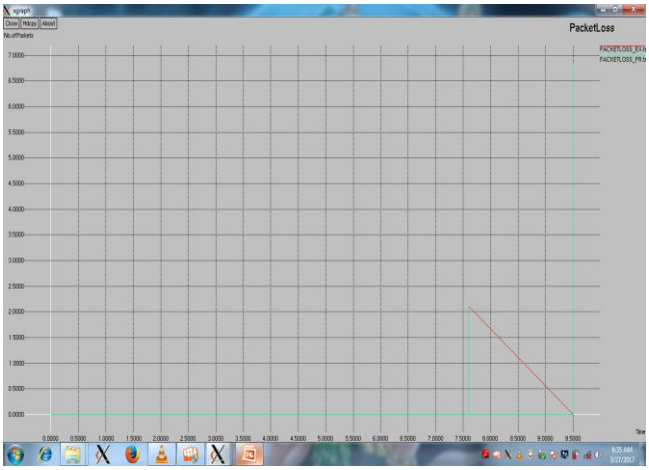

Figure 15. Packet loss graph

4. End To End Delay Graph

It is defined as time taken for a packet to be transmitted successfully across a network from source to destination. Mathematically it is defined as:

$$AED = \frac{\sum_{i=0}^{n}(t_i(r) - t_i(s))}{n_{pr}}$$

Where AED is average end to end delay $t_i(r)$ is the receiving time of packet I by the destination node, $t_i(s)$ is the sending

time of packet i by the source node and $n_{pr}$is the total number of packets received.

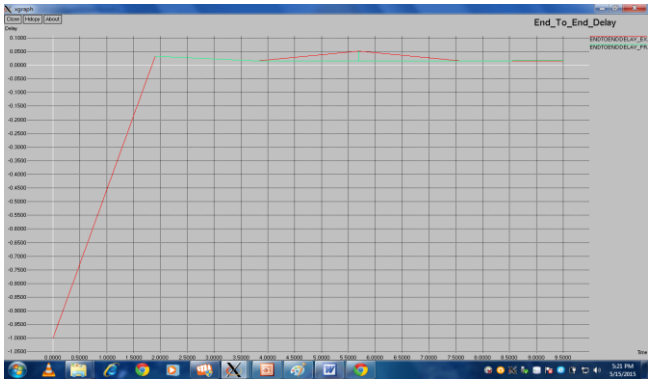

Figure 16. End-to-End Delay Graph

VI. CONCLUSION

Communication without disconnection and security are the major achievements in implementing the VANET system. In this paper, we study the proposed scheme called NTBS clustering Protocol to protect valid users in VANET and fast communication requirements and we have studied the TTR concept for giving communication requirements to the VANET system to improve the performance of the authentication procedure. The analysis calculations of proposed scheme were substantially better than in existing schemes. Moreover, NTBS clustering protocol is based on the concept of transitive trust relationships to improve the performance of the authentication procedure. Vehicular Ad Hoc Networks (VANETs) are used in wide areas of applications in recent times. Clustering of vehicles has been investigated by the research community from different perspective in many of the applications used in VANETs. The analysis provided for various existing proposals allow various users working in this domain to select one of the proposals with respect to its merits over the others.

ACKNOWLEDGMENT

I will be thankful forever to the LORD SRIRAM, BAJARANGBALI for his boundless blessings showered on me. I am very grateful and express my heartfelt countless Namaste to most respectable person Dr. S. Anathi madam ji, B.E.,M.Tech.(IISC),Ph.D.,Professor, Department of Network Systems and Information Technology, University of Madras, Guindy Campus, Chennai for their constant support, invaluable and inspiring guidance to the progress of my paper work. Without madam ji inspiration, definitely this paper work would not have been possible. I would like to express my heartfelt special thanks to most respectable, emeritus and senior Prof. (ret.) K.Padmanabhan, Former Head, CISL and Emeritus Professor in AC Technology College, Anna University for their kind support to me for carrying out this paper work. I would like to express special thanks to Prof. (ret.) Ramana Murthy M. V., Department of Mathematics & Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, and Dr. M. Raghavender sharma, HOD Department of statistics, University College of Science, Osmania University, Hyderabad, Telangana. The authors would like to thank the anonymous referees for their helpful suggestions. Finally, thanks to all who helped me directly and indirectly in carrying of this work.

REFERENCES

[1] C. Siva Ram Murthy, and B. S. Manoj, *"Ad Hoc Wireless Networks:Architectures and Protocols"*, Prentice hall PTR, 2004.

[2] Yousefi. S, Mousavi M. S, and Fathy M, *"Vehicular ad hoc networks (VANETs): challenges and perspectives"*, In the Proceedings of the 6th international conference on ITS telecommunications, pp.761-766, 2006.

[3] Kosch. T, Scroth. C, Strassberger. M, and Bechler. M, *"Automative Internetworking:The Evolution towards Connected and Coperative vehicles"*, John & Wesley Sons Ld., USA, 2012.

[4] Rasmeet S Bali, Neeraj Kumar, and Joel JPC Rodrigues, *"clustering in vehicular ad hoc networks:taxonomy, challenges and solutions"*, Vehicular communications, Vol.1, Issue.3, pp.134-152, 2014.

[5] Wenshuang liang, Zhuorong Li, and Hongyong Zhang, *"Vehicular Ad Hoc Networks:Architectures, Research Isses,Methodologies, Challenges and Trends"* Sage journals, Vol.11, Issue.8, 2015.

[6] M. Gerlach, A. Festag, T. Leinmller, G. Goldacker, and C. Harsch, *"Secure architecture for Vehicular Communications"*, 5 th international Workshop on Intellegent Transportation (WIT), March 2007.

[7] M. Raya and J. P. Hubaex, *"Securing Vehicular ad hoc networks"*, J. Compute. Security, Vol.15, Issue.1, pp.39-68, 2007.

[8] J. P. Hubaux, S. Capkun, and J. Leo, *"The Seurity and Privacy of Smart Vehicles"*, IEEE Security and Privacy Magazine, Vol. 2, Issue.4, pp.49-55,2004.

[9] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramaniam, *"Security Issues in a future Vehicular network"*, In the Proceedings of Europen Wireless'02, 2002.

[10] C. Zhang, X. Lin, R. Lu, and P. H. Ho, *"RAISE: An Efficient RSU-aided message authentication scheme in vehicular communication networks"*, In the Proceedings of the IEEE Int. Conf. Commun., pp.1451-1457, 2008.

[11] G. Gowtham, E. Samlison, *"A Secured Trust Creation in VANET Environment Using Random Password Generator"*, International Conference on Comp. Elect. And Elect. Technologies, pp.781-784,2012.

[12] T. Isaac, S. Zeadally, and J. S. Camera, *" Security attacks and solutions for vehicular ad hoc networks"*, In IET Communications, pp.894-903, 2009.

[13] Menezes, S. Vnstone, and D. Hankerson, *"Guide to elliptic curve cryptography"*, Springer Professional Computing, Springer, New York, 2004.

[14] Sirwan A Mohammad and Dr. Sattar, *"Design of wireless network based on ns2"*, Journal of Global Research in Computer Science, Vol.3, Issue.4, pp.1-8, 2012.

[15] Z. Wang, L. Liu, M. Zhou, N. Ansari, *"A position based clustering technique for ad hoc intervehicle communication*", IEEE Trans. Syst. Man Cybern., Part C, Appl.Rev. 38(2), pp.201-208, 2008.

[16] W. Fan, Y. Shi, S. Chen, L. Zou, *"A Mobility based dynamic clustering algorithm (DCA) for VANETs",* In the International Conference on Communication Technology and Application, Beijing, pp.752-756, 2011.

[17] Grzegorz Wolny, *"Modified DMAC Clustering Algorithm for VANET",* In the Procedings of the 2008 Third International Conference on Systems and Networks Communications, Washington, DC, USA, pp.268-273.

[18] Farhan ahammed, javed Taheri, and Albert Zomaya, *"LICA:Robust Localization using cluster Analysis to improve GPS Coordinates"*,

[19] Blum J, Eskandan A, Hoffman L, *"Challenges of Intervehicle ad hoc networks",* IEEE Transactions on Intelligent Transport System, Vol.5, Issue.4, pp.347-351, 2004.

[20] S. Sivagurunathan, P. Subathra, V. Mohan, N. Ramraj, *"Authentic Vehicular Environment Using a cluster based key management"*, Eur. J. Sci. Res.36,pp. 299-307, 2009.

[21] Cheng, S.-T., G.-J. Horng, and C.-L. Chou, *"using cellular automata to form car soceity in vehicular ad hoc networks"*, Intelligent Transport Systems, IEEE Transactions, Vol.12, Issue.4,pp.1374-1384, 2011.

[22] Almalag, M. S., and Weigle, M. C., *"Using traffic flow for cluster formation in vehicular ad hoc networks"*, In Local Computer Networks (LCN), 35th conference on, IEEE, pp.631-636, 2010.

[23] Souza. E, Nikolaidis. I, and Gburzynski, P. , "*A new aggregate local mobility (ALM) clustering algorithm for VANETs"* In comm. (ICC), International Conference on, IEEE, pp.1-5, 2010.

[24] Rawshdeh, Z. Y., and Mahmud. S. M, *"Toward strongly concerned clustering structure in vehicular a hoc networks"*, In Vehicular Technology Conference Fall, IEEE 70th , IEEE, pp.1-5, 2009.

[25] Shea. C, Hassanabadi, and Valaee, S., *" Mobility based clustering in VANETs using affinity propagation"*, In Global Telecommuniccations Conference, IEEE, GLOBECOM, pp. 1-6, 2009.

[26] Kayis. O., Acarman. T., *"clustering for inter vehicle communication"*, In Intelligent Transportation Systems Conference, IEEE, pp.636-641, 2007.

[27] W. Fan, Y. Shi, S.chen, and L. Zou, *"A mobility metric based dynamic clustering algorithm (DCA) for VAETS"*, in International Conference on Communication Technology and Application, Beijing, pp.752-756, 2011.

[28] Zhenxia Zhang, Azzedine Boukerche, and Richards Pazzi, *"A novel multi-hop clustering scheme for vehicular ad hoc networks"*, In the Ptoceedings of the 9th ACM international symposium on Mobility management and wireless access, ACM, pp.19-26, 2011.

[29] Mohamed Nidhal Merji, Jalel Ben-Othman, Mohamed Hamdi, *"A Survey on VANET security challenges and possible cryptographic solutions"*, Vehicular Communications, Vol.1, Issue.2, pp.53-66, 2014.

[30] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yaguang Fang, *"An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks"*, Parallel and Distributed Systems, IEEE Transactions on, Vol.21, Issue.9, pp.1227-1239, 2010.

[31] Azogu. I. K, Ferreira. M. T, and Hong Liu, *"A security metric for VANET content delivery"*, Global Communications Conference, IEEE, Vol.3, Issue.7, pp.991-996, 2012.

[32] Leinmuller T, Buttyan L et al., *"SEVECOM-Secure Vehicle Communication"*, in the Proceedings of IST Mob Summit.

[33] Zuowen, Tan , *"A Privacy Preserving Mutual Authentication Protocol for Vehiular Ad Hoc Networks"*, Journal of Convergence Inf. Technology Sciences and Engineering, Vol.5, No.1, pp.53-59, 2017.

Authors Profile

Dr. M. Raghavender Sharma pursed Bachelor of Science in Mathematics, Master of Science in Statistics, and achieved Doctoral Degree in Statistics, all degrees from OsmaniaUniversity, Hyderabad, Telangana, India. Currently he is working as vice principal and Head of the Department, Department of Statistics at University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India. He is supervising many Ph. D.'s and he has published many national, international journals. He has excellent teaching track record with 30 years teaching experience and 10 years Research experience..

Mr. Venkatamangarao Nampally (n.venkat013@gmail.com) pursed Bachelor of Science in Computer Science, Master of Science in Computer Science and Master of Technology in Computer Science & Engineering, all degrees from Osmania University, Hyderabad, Telangana, India, and pursed Master of Philosophy from University of madras, Chennai, Tamil Nadu, India. His main research work focuses on VANET communication. He has 7 years of teaching experience and 2 year of Research Experience.

