To Design Vehicular Ad-hoc Network using Sybil Attack and Optimization Technique

Samiksha[3], Iqbaldeep Kaur[2], Dr. Amit Verma[1]

[1] *Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[2] *Associate Professor Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[3] *Student Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

Abstract— The Vehicular Ad-Hoc Network, or VANET, is an innovation that uses moving cars as nodes in a network to create a mobile network. VANET turns each and every participating car into a wireless node and creates a network with a wide range. The main motive of research in VANET is to improve vehicle safety by V2V (Vehicle to Vehicle) and V2R (Vehicle to RSU) communication. The working in VANET is made similar to AODV protocol. Road side unit (RSU) is used instead of AODV protocol because it overcomes problems like jamming, intruder and traffic congestion. In Sybil attack, a malicious user of a shared network creates multiple fictitious identities and utilises their combined influence to sidestep the reputative system. The optimization technique used in this is Artificial Bee Colony which is an improved optimization technique which simulates the intelligent search behaviour of honey bees.

Keywords— VANET; RSU; Intruder; AODV; Sybil Attack

I. INTRODUCTION

VANETs can be exploited for a wide range of safety and non-safety applications, allow for additional services such as vehicle safety, automatic toll payment, traffic management, improved navigation, location based services. Vehicular Ad-hoc Networks (VANETs) signify a rapidly evolving, primarily challenging class of MANETs. VANETs are distributed, self-establishing communication networks assembled by moving vehicles, and are hence characterized by limited freedom in the mobility patterns and very high node mobility [2].

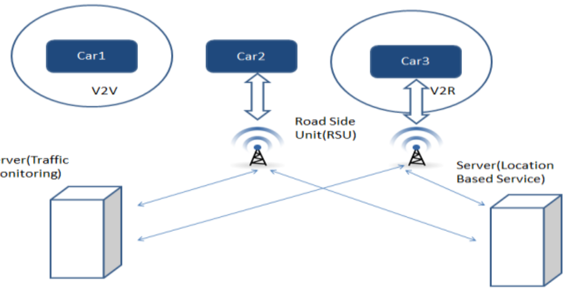

Fig.1: VANET Architecture

A VANET system may consist of these three types of Communication categories:

A. Intelligent transportation systems

In intelligent transportation systems, each vehicle contains sender, receiver, and router to transmission info to the vehicular network or transportation activity, which then uses the information to guarantee safe, free-flow of traffic [18]. For communication which has to be occur between vehicles and Roadside Unit vehicles must be prepared with some sort of radio interface [4].

B. Inter-vehicle communication

The inter-vehicle communication conformation figure no: 1 uses multi-hop multicast or program to transmit traffic correlated information over multiple hops to a group of receivers.

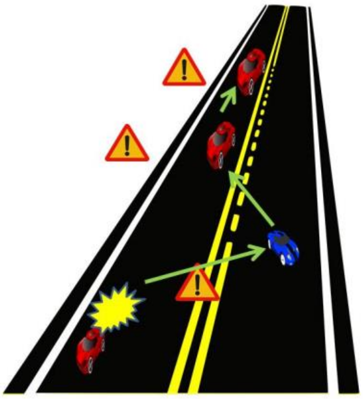

Fig.2: Intelligent Transportation System

C. Vehicle-to-roadside communication

The vehicle-to-roadside communication formation characterizes a single hop broadcast where the roadside unit sends a broadcast message to all prepared vehicles in the vicinity [11]. Vehicle-to-roadside communication formation provides a high bandwidth link between automobiles and roadside units [7].The roadside units may be placed every kilometre or less, succeeding high data rates to be continued in heavy traffic.

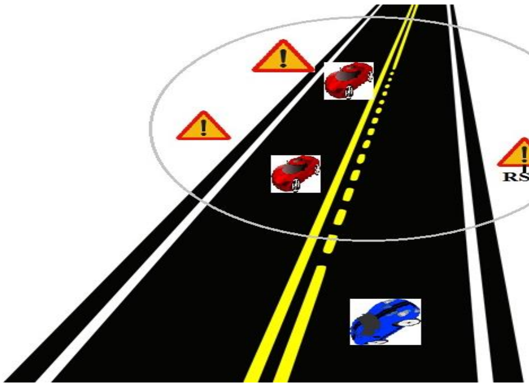

Fig.3: Vehicle to roadside Communication

D. Routing-based communication

The routing based communication arrangement is a multi-hop unicast. Routing based announcement hop fashion until the vehicle carrying the anticipated data is reached [8][9].When the request is received by a vehicle preserving the desired piece of information instantly sends a unicast message containing the information to the vehicle it established the request from, which is then exiting with the task of forwarding it towards the query source [20].

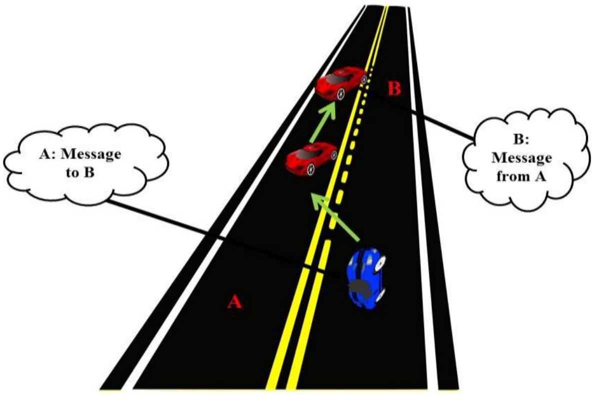

Fig.4: Routing based Communication

E. Security Requirements In Vanet

There are main three security requirements in VANET. These are as follows:

Confidentiality: In VANETs, confidentiality refers to "confidential communication" . In a group, none except group members are able to encode the messages that are broadcasted to every member of group and none (even other members) except a dedicated receiver member is capable to decode the message devoted to it.

Integrity: It ensures that messages conveyed among nodes are not altered by the attackers. This concept in VANETs ensure that: A node should be able to verify that a message is in reality sent and hence signed by another node without being modified by anyone. For this, Data Verification is also required.The receiving vehicle performs data verification to check whether the message is same or not, once the sender vehicle is authenticated.

Availability: If the network is under an attack then it should be available without affecting its performance .This concept of VANETs is not easy to ensure because of the mobility in vehicles.

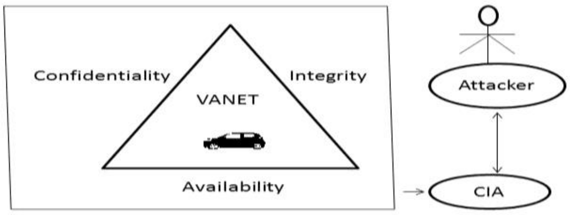

Fig.5: Security Requirements

II. CHALLENGES IN VANET

Technical Challenges

- Network Management: We cannot use structures like tree because these structures cannot be set up and maintained as rapidly as the topology changed due to high mobility.
- Environmental Impact: For communication in VANET electromagnetic waves are used. These waves are influenced by nature. Thus to send the VANET the ecological effect must be considered.
- Security: In VANET, security is mainly concerned . So transmission of messages must be secured. For this VANET must provide security applications so that messages must be transmit safely.
- Congestion and collision Control: The greatest challenge is unbounded network size . The traffic load is low in urban areas at night and in rural areas in day . Due to this, the system segments every now and again happens while in surge hours the activity burden is high and so the subsequently system is congested and crash happens in the system.

Security Challenges

- Real-time constraints: Real-time constraints should be maintained since vehicles can arbitrarily move in and quickly move out to a group of a VANET for a short duration.
- Low tolerance for error: On the basis of probability, some protocols are designed. VANET uses such life critical information on which activity is performed in brief time. A little blunder in probabilistic calculation may bring about mischief.
- Key Distribution: In VANET , all the security mechanisms implemented dependent on keys. Every message is encoded and need to unscramble at collector end either with same key or diverse key. Therefore key distribution

among vehicles has become a major challenge in designing a security protocol.

- Mobility Modeling: keeping in mind the end goal to execute VANET proficiently and reasonably, an exact versatility model is required for this very dynamic environment of VANET.

III. CHARACTERISTICS OF VANET

- Rapidly Changing Network Topology: The network topology in VANETs changes frequently, due to high node mobility.
- Unbounded Network Size:The VANETs network should not be dependent on the number of the nodes as VANETs could involve the vehicles in one city, several cities, or even a country .
- Potential Support from Infrastructure: Unlike MANETs, VANETs can really take advantage of infrastructure in the future. This property must be considered to make any protocols and plans for VANETs betterment.
- Abundant Resources: The VANET nodes have computation resources and abundant vitality. This takes into consideration of plans including utilization of resource demanding techniques, for example, ECDSA, RSA, and so forth.
- High Mobility: The nodes (vehicle) in VANETs typically moves at rapid speed. The node motion is compelled by the road topology and its layout.
- Delay-sensitive Data Exchange: In VANETs , the message should be transfer without any delay because security related application need message conveyance immediately.
- Better Physical Protection: VANET nodes are more difficult to compromise, which is also good news for security in VANETs. Nodes in VANET are better protected than those nodes in other MANETs.

IV. ATTACKS IN VANET

1) DOS Attack

In this type of attack , the attacker prevents the true user to use the service from the sufferer node. DOS attacks are most conspicuous attack DOS attacks can be carried out in many ways :

a) Jamming: In this technique the attacker detects the physical channel and gets the information about the recurrence at which the receiver receives the signal. At that point he transmits the signal on the channel with the goal that channel is jam.

b) Distributed DOS attack: The another form of DOS attack is DDOS attack. In this attack, multiple attackers attack the sufferer node and prevents true user from accessing the service.

c) Ping flooding is the most secondary form of DOS attack since anybody can do it to a great degree effortlessly. The PC's system gets to be moved down, attempting to stay aware of ping when a targeted PC is under a ping flood attack .Every time the server receives a ping request it has to compute it then send a reply with the same amount of data.

2) Eavesdropping: It is the most common attack on confidentiality. The main goal of this attack is to get entrance of the confidential information. This attack belongs to network layer attack and is passive in nature.

3) Session hijacking: At the start of the session , the certification process is done. In this attack , the attacker takes the control of session between the nodes. Hence it is easy to hijack the session after the connection is established.

4) Identity revealing: In this attack , the attacker can reveal the identity of the driver as he himself is the owner of his vehicle.Thus our privacy is at risk.

5) Black Hole attack: In this attack, the attacker attracts the nodes to transmit the packet through itself. It can possible be done by consistent sending the malicious route reply with fresh route .After attracting the node, it silently drops the packet when the packet is forwarded through this node.

6) Gray Hole attack: This is the augmentation of black hole attack. In this attack, the malicious node behaves like the black node . In this, it drops the packet selectively. This selection can be done by two ways:

i) The malicious node can drop the packet on the basis of probabilistic distribution.

ii) A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.

7) Global Positioning System (GPS) Spoofing: It keeps up an area table with the geographic area and personality of all vehicles on the system. An attacker can trick vehicles into feeling that they are in a distinctive area by creating false readings in the GPS situating system devices.

8) Sybil Attack

In Sybil attack , multiple messages are sent from the attacker node with multiple identities. Consequently, the attacker recreates several nodes in the network. The goal of these attacks might be basically to give figment of a congested driving condition to constrain different vehicles to leave the road for the benefit of the attacker. Sybil attacks are always possible except under extreme and unrealistic assumption of resource parity.

Routing Protocol in VANET

These procedures discover the way & maintain it in a table before the sender starts transmitting data. They are further separated into Proactive, Reactive & hybrid procedures [12].

a)Proactive protocols

The proactive protocol is also known as table driven routing protocol [13]. These protocols work by periodically exchanging the knowledge of topology between all the knobs of the network. The positive protocols do not have initial route discovery delay but consumes lot of bandwidth for intermittent apprises of topology. There are some routing protocols that decrease under this category [14].

b) Reactive protocols

These protocols are named as on-demand routing protocols as they occasionally update the defeating table, when several data is there to refer. But these protocols use flooding process for route discovery, which reasons more steering overhead & also agonize from the primary route discovery process, which create them unsuitable for safety applications in VANET.

c) Hybrid protocol

HRP is a hybrid protocol that divides the system into several zones, which makes a hierarchical protocol [15] as the protocol ZHLS (zone-based hierarchical link state). HRP is based on GPS (Global positioning system), which permits every knob to identify its physical position before mapping an area with table to recognize it to which it fits. The amount of messages exchanged in high ZHLS is what influences the profession of the bandwidth. Our procedure efforts to decrease the number of messages exchanged, thus increasing network performance and service life.

IV. CURRENT WORK

Sybil Attack

Sybil attack works in peer-to-peer network by creating false identities of a reputed system. Sybil attack creates false identities very fast which ruins the reputed network. An entity is a piece of software which has access in local resources. Entity is represented as identity [13]. More than one identity can relate to a single entity. The identity is used as a reflection so that remote entity can know about the identities without essentially knowing the correspondence of identities to nearby entities [19]. As a matter of fact, each distinct identity is usually accepted to relate to distinct local identity. In reality many identities may correspond to the same local identity. Sybil attacks have been showed up in many scenarios, with wide implications for security, safety and trust [14]. For example, an internet poll can be fixed using multiple IP addresses to submit a large number of votes. Some companies have also used Sybil attacks to gain better ratings on Google Page Rank. Reputation systems like eBay's have also been victims of this type of attack.

Sybil Attack can do the following:

•The Sybil attack can defeat replication and discontinuity mechanisms in peer-to-peer systems [15].

•The Sybil attack can be utilized against routing algorithms in sensor networks.

•By using the Sybil attack, one malicious node might have the capacity to contribute to the aggregate many times.

•Wireless sensor networks use voting for a number of tasks. The Sybil attack could be used to “stuff the ballot box” in any vote.

•In Sybil attack, a malicious node can be utilized to obtain an unfair share of any resource shared [16][17].

Road side unit or sensor

Roadside sensor nodes measure the road condition at several positions on the surface, collective the measured standards & communicate their amassed value to an approaching vehicle. The vehicle generates a cautionary message & dispenses it to all automobiles in a certain geographical region, potentially using wireless multi-hop statement. For post-accident examination, sensor nodes continuously measure the road condition and supply this info within the WSN itself. When a coincidence occurs, road condition data stored over a sufficiently long period can be used for criminal modernization of road accidents. In difference to the accident deterrence service, such an accountability service requirements to be constrained to a well specified group of end-users, e.g. insurance companies or the road patrol [16]. Information stored inside the WSN can likewise be utilized to judge a driver’s driving style according to the road condition at the moment of an accident.

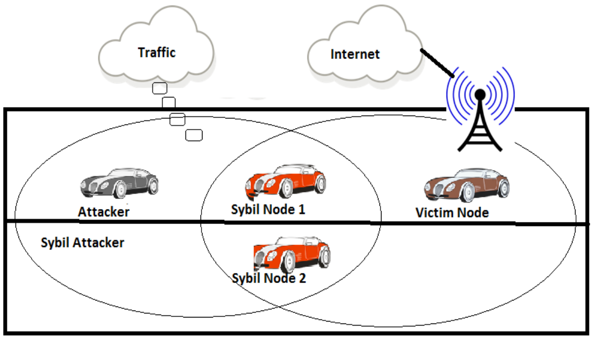

Fig.6: Sybil Attack

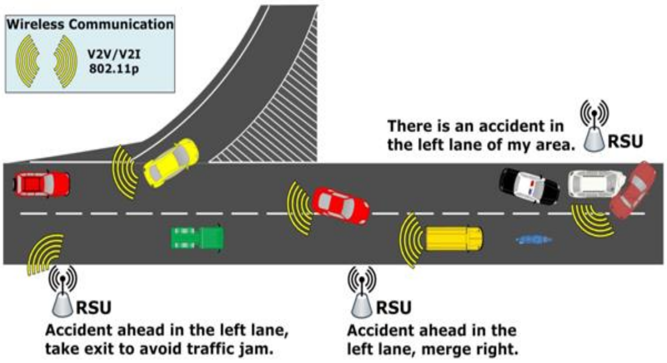
Wireless Communication
V2V/V2I
802.11p
There is an accident in the left lane of my area.
RSU
RSU
Accident ahead in the left lane, take exit to avoid traffic jam.
RSU
Accident ahead in the left lane, merge right.

Fig.7: Road Side Unit

AODV (Ad-hoc on demand Distance Vector) Routing Protocol

Is a source initiated routing protocol & usages HELLO letters to recognize its neighbors? Source node broadcasts a route request to its neighbors which fill forward to the destination. Then the terminus unicast a route response packet to the sender. Each node preserves broadcast-id which increases for new RREQ. When a RREQ arrives at a knob, it checks the broadcast id if it is minus than or alike to previous memo then it will discard the packet.
AODV protocol mainly involves 3 packets. They are:
1. The route request (RREQ) is mainly used for the establishment of packets from source to destination.

2. The route reply (RREP) is sent by the destination to the source after the establishment of route.
3. The route error (RERR) is sent by intermediate node or destination in 2 conditions. When there is no path to the destination. When the link breaks in the valid path to the destination.

V. PROMINENT ALGORITHMS

Artificial Bee Colony is based on the model first proposed by Karaboga. It is a swarm based and metaheuristic algorithm and is very simple , robust and population based optimization algorithm.The performance of ABC algorithm is compared with other well-known modern algorithms such as Differential Evolution(DE) , Genetic Algorithm(GA) on constrained and unconstrained problems.ABC is an iterative process. The fundamental calculation of ABC is moderately basic and its usage is clear to solve the streamlining issues. ABC has been observed to be exceptionally successful having the capacity to create great results at a low computational expense.

The performance of ABC algorithm is tested on XOR , 3-Bit parity benchmark problems and Decoder-Encoder.
To find the cluster head, the ABC algorithm employs a population of bees. With reference of ABC , the potential solutions are food sources of nectar bees.In terms of quality of food sources , the fitness is determined.
ABC algorithm consists of three groups of artificial bees.
Employed Foragers
Onlookers
Scouts
The first half of the colony consists of the Employed bees whereas the second half consists of onlookers.
The Employed bees are linked to a particular food sources i.e number of employed bees is equal to number of food sources.
To select a food source , the onlookers observe the move of the employed bees inside the hive , .
Scouts search randomly for new food sources.

ABC Cycle consists of three rules which are as follows :
-Sending the employed bees to a food source and evaluating the nectar quality.
-After obtaining information from the employed bees , the onlookers choose the food sources and calculate the nectar quality.
-Determining the scout bees and sending them onto the possible food sources.

Algorithm_ABC

```
Step 1: Initialize the ABC algorithm and issue parameters $F_{sm}$
//Where $F_{sm}$ is Food Source Memory.
Step 2: repeat
      Transmit $E_{bfs}$
      //Where $E_{bfs}$ employed bees to the food sources
       Transmit $O_{cfs}$
      //Where $O_{cfs}$ is onlookers to choose a food source
Step 3: Memorize the best nourishment food source
         End
```

Algorithm 1: Pseudo code of ABC Algorithm

In the initialization phase, an artificial scout bees and control parameters initialize the population of food sources.

In the employed bees phase, artificial employed bees look for new food sources having more nectar inside the area of nourishment food source in their memory. The calculation of its fitness is done after finding a neighbour food source. After that, the information of employed bees is shared with onlooker bees waiting in the hive by dancing on the dancing area.

Algorithm_Employed bees

```
Step 1:
        for
           {
              $j = 1…SN$   do
Step 2:          for
                 {
                     $i = 1…N$   do
                 }
             }
Step 3:  $x'(i) = x_j(i) \pm r(x_j(i)) - x_k(i)$ ,
              // $\forall k \in (1,2,,,,,SN),\ k \neq j$ and $r \sim (0,1)$
Step 4:  end for
Step 5:                    Calculate $f(x_i)$
Step 6:                         if
                                  $(f(x') \leq f(x_i))$      then
Step 7:                            $x_i = x'$
Step 8:                                       $f(x_i) = f(x')$
Step 9:                                              end if
Step 10: end for
```

Algorithm 2 :Employed bees phase

In the onlooker bees phase, depending on the information provided by the employed bees , artificial onlooker bees probabilistically choose their food sources. For this, a technique can be used known as fitness based selection technique. After this,a neighbourhood source is determined and its fitness value is computed.

Algorithm_ Onlookers

```
Step 1:
           for  i=1…$SN$  do
                {
                                            //Where  $r \sim (0, 1)$
Step 2:             sum_prob = 0
Step 3:                    Initialize j=0
Step 4:                     while (sum_prob ≤ r) do
Step 5:                      $sum\_prob = sum\_prob + p_j$
Step 6:                         j=j+1
Step 7:              for  k = 1…N  do
                       {
Step 8:                 $x'(j) = x_j(k) \pm r(x_j(k) - x_j(m)$,
                      $\forall m \in (1, 2, …..,SN)$
Step 9:          end for
                  }
Step 10:              Calculate $f(x_j)$
Step 11:                if ($f(x') \leq f(x_j)$) then
Step 12:                    $xj = x'$
Step 13:                      $f(x_j) = f(x'_j)$
Step 14:                end if
Step 15:   end for
             }
```

Algorithm 3 : Onlooker bees phase

In the scout bees phase, utilized honey bees whose arrangements can't be enhanced through a foreordained number of trials, called "limit", get to be scouts and their answers are deserted.

Then, the scouts start to search for new solutions randomly. Thus, those sources which are at first poor or have been made poor by abuse are deserted and negative criticism conduct emerges to adjust the positive input.

Algorithm_ Scout bees

```
Step 1:
        for $i = 1 \ldots SN$ do
            {
Step 2:         if (scout(i) = limit) then
Step 3:               Generate $x_j$
Step 4:         end if
Step 5:  end for
            }
```

Algorithm 4 : Scout bees Phase

These three stages are rehashed until an end criteria is fulfilled.

General features of Intelligent Swarm

Positive criticism: advancing the making of advantageous structures. Enrolment and fortification, for example, trail laying and following in some insect species can be appeared as case of positive criticism.

Negative criticism: counterbalancing positive input and balancing out the system design. Keeping in mind the end goal to stay away from the immersion which may happen as far as accessible foragers a negative criticism instrument is required.

Multiple interactions: Agents in the swarm utilize the information originating from the other agents so that the information spreads throughout the system.

Fluctuations: Arbitrary strolls, mistakes, irregular assignment exchanging among swarm people which are key for innovativeness. Arbitrariness is frequently noteworthy for developing structures since it empowers the disclosure of new arrangements.

VI. SCOPE

VANET has some unique features which make it dissimilar from MANET as well as stimulating for designing VANET applications.

•High dynamic topology

The topology of VANET variations because of the movement of automobiles at high speed. Suppose two vehicles are moving at the speed of 20m/sec & the radio range amongst them is 160 m. Then the link between the two vehicles will last 160/20 = 8 sec .

•Frequent disconnected network

From the highly dynamic topology results we observe that frequent disconnection occur amongst 2 vehicles when they are replacing information. This disconnection will occur most in sparse network .

•Mobility modelling [9]

The mobility pattern of vehicles depends on traffic environment, roads structure, the speed of vehicles, driver's motivating behavior & so on.

•Battery power and storage capacity

In modern vehicles battery power & storage is indefinite. Thus it has sufficient computing power which is unavailable in MANET. It is helpful for effective communication & making routing decisions.

•Communication environment

The communication environment between vehicles is dissimilar in sparse system & dense system. In dense network building, trees & other objects behave as obstacles & in sparse system like high-way [10] this equipment are absent. So the routing approach of sparse & dense network will be different.

VII. REFERENCES

[1]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on. IEEE, 2010.

[2]. X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[3]. Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011

[4]. Schmidt RK, Leinmuller T, Schoch E, Held A, Schafer G (2008) Vehicle behavior analysis to enhance security in vanets. In:Workshop on vehicle to vehicle communications.

[5]. C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in Proc. 27th IEEE INFOCOM, Phoenix, AZ, USA, 2008, pp. 246–250.

[6]. M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[7]. X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications,"

IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[8]. C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE ICC, Beijing, China, May 2008, pp. 1451–1457.

[9]. Dotzer F, Fischer L, Magiera P (2005) Vars: a vehicle ad-hoc network reputation system. In: IEEE international symposium on a world of wireless mobile and multimedia networks,pp 454–456.

[10]. Liu, Yue, Jun Bi, and Ju Yang. "Research on vehicular ad hoc networks."Control and Decision Conference, 2009. CCDC'09. Chinese. IEEE, 2009.

[11]. Kakarla, Jagadeesh, S. Siva Sathya, and B. Govinda Laxmi. "A survey on routing protocols and its issues in VANET." (2011).

[12]. Asaju La'Aro Bolaji, Ahamad Tajudin Khader, Mohammed Azmi Al-Betar and Mohammed A. Awadallah," ARTIFICIAL BEE COLONY ALGORITHM, ITS VARIANTS AND APPLICATIONS: A SURVEY" in Journal of Theoretical and Applied Information Technology (2013).

[13]. Dervis Karaboga, Celal Ozturk,"A novel clustering approach: Artificial Bee Colony (ABC) algorithm" Applied Soft Computing (2011).

[14]. Dervis Karaboga, Beyza Gorkemli,Celal Ozturk,Nurhan Karaboga,"A comprehensive survey: artificial bee colony (ABC) algorithm and applications" in Springer Science+Business Media B.V.(2012).

[15]. Dervis Karaboga,Selcuk Okdem,Celal Ozturk,"Cluster based wireless sensor network routing using artificial bee colony algorithm" in Springer Science+Business Media, LLC (2012).

[16]. Subramaniam, Prabhakar Rontala, Arunkumar Thangavelu, and Chitra Venugopal. "QoS for highly dynamic Vehicular ad hoc network optimality."ITS Telecommunications (ITST), 2011 11th International Conference on. IEEE, 2011.

[17]. Zheng, Liming, Wanlei Li, and Bo Xie. "Research on Communications over VANET under Different Scenes and Implementation of Vehicle Terminal."Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on. IEEE, 2012.

[18]. Barnwal, Rajesh P., and Soumya K. Ghosh. "Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks." Connected Vehicles and Expo (ICCVE), 2012 International Conference on. IEEE, 2012.

[19]. Hussain, Rifaqat, et al. "Rethinking vehicular communications: Merging VANET with cloud computing." Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. IEEE, 2012.

[20]. Baldini, Gianmarco, et al. "Identity-based security systems for vehicular ad-hoc networks." Connected Vehicles and Expo (ICCVE), 2013 International Conference on. IEEE, 2013.