I J C T A, 9(34) 2016, pp. 43-55

To Design the Trust Management System using Road Side Unit and Artificial Bee Colony Technique based on Vehicular Ad-hoc Network

[1]Amit Verma, [2]Samiksha and [3]Iqbaldeep Kaur

ABSTRACT

To design and implement a wireless vehicular ad hoc network for future testing by implementing SYBIL Attack to check its impact on Multipath routing in VANET by comparing the parameters like throughput, packet delivery rate by an optimization technique. There are different kinds of methods which have been adapted by researchers for analysis of data. On the basis of their different parameters each method varies. These methods are implemented on MATLAB tool. The issue gets to be making an upgraded directing convention which gives multipath disclosure and controlled traffic load in vehicular ad-hoc network. At whatever point a connection or a course break happens, a course recovery is performed which thusly importunes the backup way to go choice from the accessible hubs on the premise of the neighbouring hub which is first to send course answer bundle from goal if there are more than 1 handle sending bundle at same time then handle with higher accessible data transfer capacity will be chosen. Henceforth the general issue of this thesis work is to keep the system from substantial burden happened because of Sybil attack at the system server. To handle this, there is a need to apply an optimization technique known as Artificial Bee Colony (ABC) to prevent and save the information in particular nodes.

Keywords: VANET, RSU, ABC, Intruder, Sybil Attack

1. INTRODUCTION

Vehicular Ad Hoc Networks have created out of the need to arrangement the developing number of remote delivers that can now be utilized as a part of vehicles. These produces incorporate remote keyless passage gadgets, individual advanced supporters, tablets and portable handsets. As versatile remote gadgets and systems turn out to be continuously imperative, the interest for Vehicle-to-Vehicle and Vehicle-to-Roadside or Vehicle-to-Infrastructure Communication will stay to develop [2]. VANETs can be misused for an expansive assortment of wellbeing and non-security applications, consider esteem extra administrations, for example, vehicle security, programmed toll installment, movement administration, enhanced route, area based administrations, for example, conclusion the nearest fuel area, diner or travel lodge and infotainment entries, for example, long as access to the Internet.

VANET is normally part Movable Ad-hoc system. Vehicular Ad-hoc System is mixture of Ad-hoc System & sensing System. In Vanet, automobiles act as sensing's which container interchange data between each other deprived of any infra-structure System created. Directional mobility & high dynamic of the

[1*] Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India, *E-mail: Dramitverma.cu@gmail.com*

[2] M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College, Landran, Punjab, *E-mail: samikshakmr16@gmail.com*

[3] Associate Professor, Computer Science & Engineering, Chandigarh Engineering College, Landran, Punjab, *E-mail: iqbaldeepkaur.cu@gmail.com*

Automobiles are significant characteristics. In order to contribute in such a system, a vehicle has been prepared with a superior electric instrument which will give ad hoc system connectivity for the automobiles. VANETs are continuously shaped between affecting Automobiles prepared with wireless interfaces that might have dissimilar & same wireless boundary tools, employing less range to intermediate range message system. The best instance of VANET is Transport System of one travel support or any company which is merged internally. This Transport System of an Automobiles are influencing in any parts of city and different courses to pick or drop customer or specialists on the off chance that they are related together, which make an Ad hoc System and connected wireless.

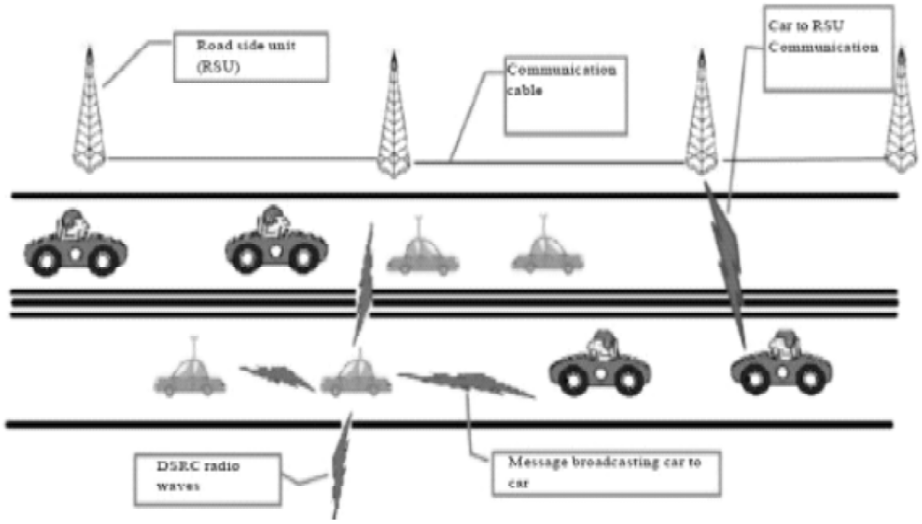


Figure 1: Vehicular Ad-hoc Network

The uses of VANETs into taking after classes:

1. Real-time program: The continuous activity information can be put at the RSU & can be available to the Automobiles at whatever opinion & anywhere required.
2. Co-agent Communication Transmission: Deliberate/Stationary Automobile with skill communications & co-work to help dissimilar automobiles. Despite the fact that unwavering quality & dormancy would be of important worry, it may systematize clothes comparable catastrophe decelerating to dodge probable mischances. So likewise, crisis microelectronic constraint light might be added suggestion.
3. Post-Crash Announcement: An automobile included in a mishap would transmission cautionary communications around its location to sprawling automobiles with the goal that it canister revenue choice by period under regulator & moreover to the superhighway watch aimed at pull absent backing by way of portrayed.
4. Road Hazard Regulator Announcement: Coaches counselling different autos around street consuming avalanche & data with respect to street highpoint warning since of street twist, unexpected downhill & so forth.
5. Cooperative Collision Warning: Signals two drivers believably under coincidence course with the goal that they can patch their ways.
6. Faraway Automobile Personalization/ Diagnostics: It benefits in transferring of customized automobile locations or transferring of automobile diagnostics after/to base.
7. Internet Admittance: Automobiles can become to web done RSU if RSU is filling in switch.

8. Digital leader transferring: Chart of settings canister is transferred by the motorists according to the prerequisite beforehand making a trip to additional region for portable course. Likewise, Gratified Chart Database Transfer goes about as an entryway aimed at receiving lucrative data from multipurpose problem parts or home-produced.
9. Actual Time Film Communicate: On-interest film knowledge won't be controlled to the boundaries of the household & the motorist can request continuous feature transfer of his most loved motion images.
10. Value-included ad: This is mainly for the administration suppliers, who need to pull in clients to their provisions. Statements similar gas pumps, roadways eateries to declare their administrations to the teamsters inside communiqué collection. This submission can be reachable even without the Internet.
11. Parking Availability: Notifications with respect to the availability of stopping in the municipal urban communities serves to discover the accessibility of openings in parking garages in a certain topographical territory.
12. Active Prediction: It expects the forthcoming geography of the street, which is required to improve fuel utilization by modifying the cruising speed before beginning a plunge or a climb. Besides, the driver is likewise helped.
13. Period Operation: If a voyager transfers his message, he can change bottleneck movement hooked on a profitable undertaking & recited on-load up framework & recited it himself if movement.

2. CURRENT WORK

There are several fashionable ideas, such as those networks can be secured by encryption & that systems can be protected by firewalls. The best place to start debunking these notions may be to seem at the most general attacks. Of course, lots of attacks are presented in the media as network hacking when they are actually done in more traditional ways [6]. To launch attacks alongside networks & network strategy the threats use a variety of tools, scripts, and programs. Typically, the network devices under attack are the endpoints, such as servers and desktops.

Sybil attack refers to the many copies of malicious knobs. It can be occur, if the spiteful node shares its surreptitious key with further spiteful knobs. This way the figure of malicious node is improved in the system & the prospect of the attack is as well increased. If we apply the multipath routing, then the option of deciding a path in the system, those enclose the spiteful node will be increased.

Vehicular system is a precise kind of mobile ad hoc network that are movable anywhere and are substituted with automobiles arranged with on boarding unit communication devices [10]. VANETs have particular diverse features in decision with MANETs counting quick alteration in topology, no power limitation, great scale, adjustable network compactness and high expectable agility. VANET construction is calculated for vehicle to automobile and automobile to organization communications with two statement devices so-called the Curb Unit that is situated on the roadside and OBU installed in automobiles. It also requirements to some sensors connected on the vehicles for meeting conservational and road information. The halfway utilized for transportations in the midst of vehicles is 5.9 GHz Ardent Short Range Announcement distinguished as IEEE 802.11p. Unpaid to remote associations, VANETs are obligated to a large portion of the security attacks. One of the injurious attacks is Sybil attack familiarized by Douceur. In this attack, one invader creates multiple features either by counterfeiting new individualities or stealing eccentricities from adjacent vehicles. Stashing personalities can happen by catching attributes in message course, as vehicles inside the statement scope of sender can spy its traded messages. There are frequent wicked processes by Sybil attackers in assorted milieus that two chief indemnities by aggressor are:

a) Direction-finding

Attacker can interrupt steering protocols in VANET. Two direction-finding appliances defenseless to the Sybil attack are multi track routing and structural direction-finding. Additionally, Sybil attack can also interrupt the crown collection instrument of numerous cluster based routing protocols. In multi path overwhelming, a set of tracks that seem detached may pass over the Sybil nodes owned by a spiteful node. In topographical overpowering protocols, malicious knobs may appear at extra than one place at a time.

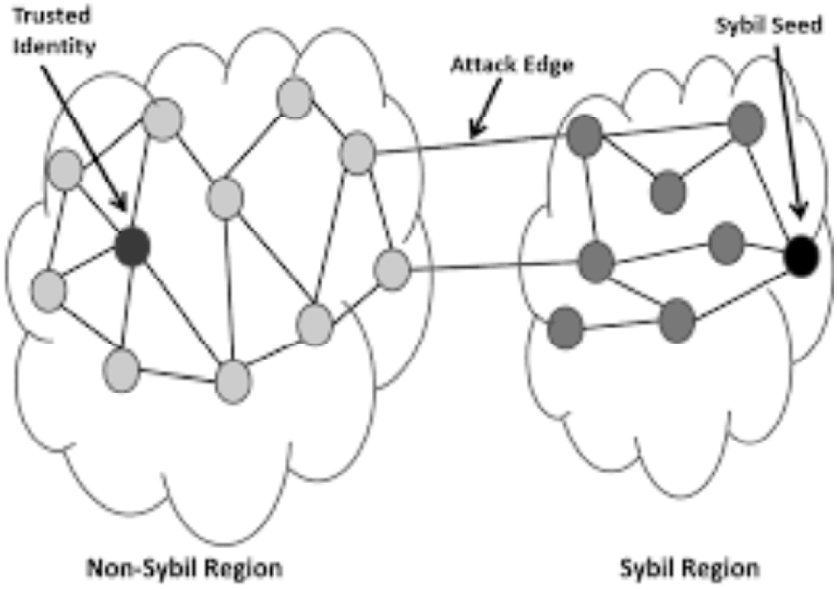


Figure 2: Direction Finding

b) Voting and Standing Organizations

The optional is an actual for congregation and proving some beneficial gen for countless of offers those Sybil nodes can modification elective outcome. Reporting and identifying node misconduct and verifying vehicle location are specimens of elective requests. Due to great impairment when this dose occurs, we ought to have an efficient method for detecting Sybil attack. Resistance instrument for practical employment should have proper discovery rate, minimal time difficulty, arrangement discretion of motorists and as much as conceivable not growth switching messages in the system. So in this every day we examine different apparatuses for Sybil attack uncovering and then rapid some of the certain investigation works with their geographies, rewards and shortcomings.

Vehicular extra on interest directing produces overwhelming steering activity by indiscriminately flooding the whole framework with RREQ parcels amid course location. The steering over vehicular advertisement connected with spread of directing bundles is very tremendous particularly when topology adjustments. Multipath steering conventions reserve various courses to a goal in a solitary course disclosure. Nonetheless, in nearness of portability, multipath conventions bring about vehicular extra bundle drops and defer because of their reliance on conceivably stale courses from stores Protocols utilizing either constrained vehicular advertisement cast or neighborhood recuperation have concentrated on lessening parcel drops and not on using the data transfer capacity effectively amid course recuperation.

Hence the overall problem of this research work is to prevent the network from heavy load occurred due to Sybil attack at the network server. The evaluation of QOS parameters like throughput, end to end delay, and network load and packet delivery rate are also included in this thesis work.

3. IMPROVED ALGORITHM

3.1. Road Side Unit (RSU)

Roadside sensor hubs measure the street condition at a few positions at first glance, aggregate the deliberate principles and impart their amassed worth to a drawing closer vehicle. The vehicle creates a preventative message and administers it to all autos in a specific land locale, possibly utilizing remote multi-jump proclamation. For post-mischance examination, sensor hubs consistently measure the street condition and supply this data inside the WSN itself. At the point when a happenstance happens, street condition information put away over an adequately long stretch can be utilized for criminal modernization of street mishaps. In distinction to the mishap prevention administration, such a responsibility administration prerequisites to be obliged to a very much determined gathering of end-clients, e.g. insurance agencies or the street watch [16]. Data put away inside the WSN can in like manner be used to judge a driver's driving style as indicated by the street condition right now of a mishap.

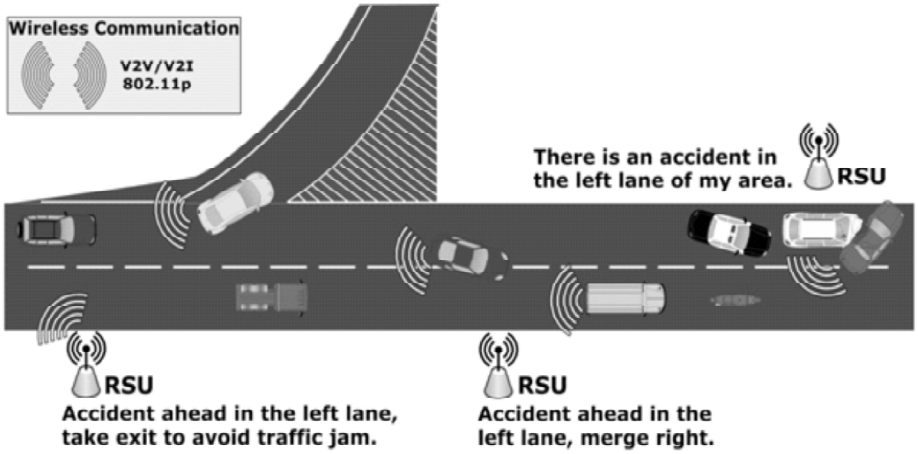


Figure 3: Road Side Unit (RSU)

3.2. Artificial Bee Colony (ABC)

An artificial honey bee comprises of working honey bees, onlookers and scouts. A honey bee coming up on the move zone to acquire the data about nourishment sources is known as an observer, a honey bee setting off to the sustenance source is named as an utilized honey bee, and a honey bee doing unintentional hunt is known as an aide. The area of a nourishment source indicates a conceivable answer for the enhancement issue, and the nectar measures of a sustenance source speak to the nature of the associated arrangement. At first, a haphazardly conveyed populace is creating. For each nourishment source, there is one and only working honey bee. So the quantity of working honey bees is equivalent to the numeral of nourishment sources.

A short time later, the positions will be overhauled more than once with the consequent cycles until the greatest reiteration is come to or stop conditions are fulfilled. Each utilized honey bee ceaselessly recalls its past best area, and produces another position inside its territory in its memory. As per the covetous standard, the utilized honey bee advises its nourishment source. At the end of the day, when the new sustenance source is better, the old nourishment source position is modernized with the new one. After every working honey bee complete their hunt procedure; they partition the data about the course and reserved quality to sustenance sources and the nectar sums with spectators by means of a purported waggle move in the moving range.

By the reflection on the waggle move, every spectator picks a sustenance source contingent upon the likelihood esteem associated with the nourishment source, and hunts the region inside its area to produce

another hopeful arrangement. And after that, the avaricious foundation is utilitarian again pretty much as it works in the working honey bees [21]. In the event that a position can't be improved after a foreordained number of cycles, the position ought to be dumped; in the meantime, the resultant utilized honey bee changes over a scout. The relinquished position will be traded with another indiscriminately produced sustenance source [13].

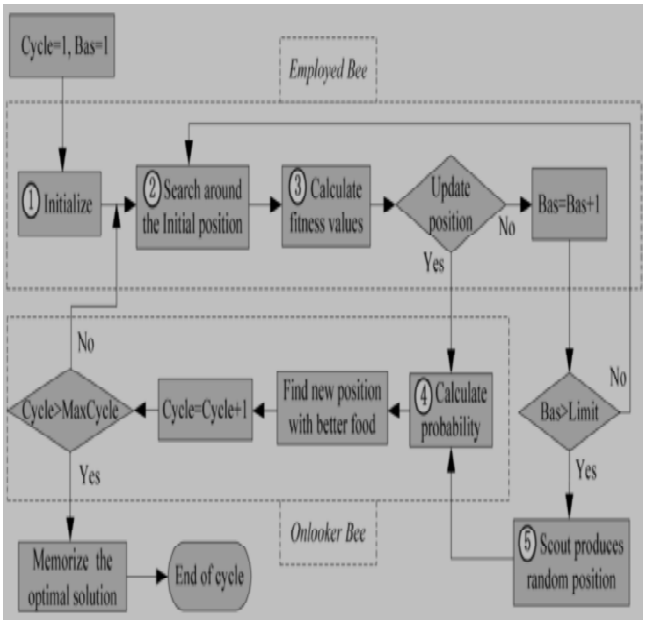


Figure 4: ABC Algorithm Flowchart

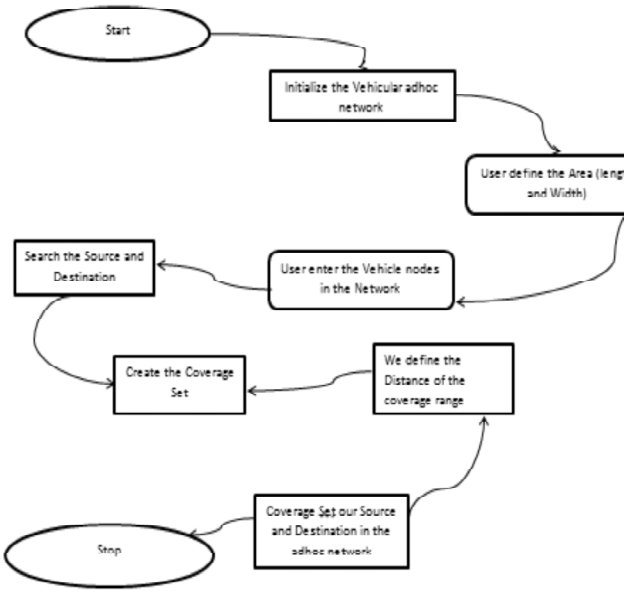


Figure 5: Data Flow Diagram (Level 0)

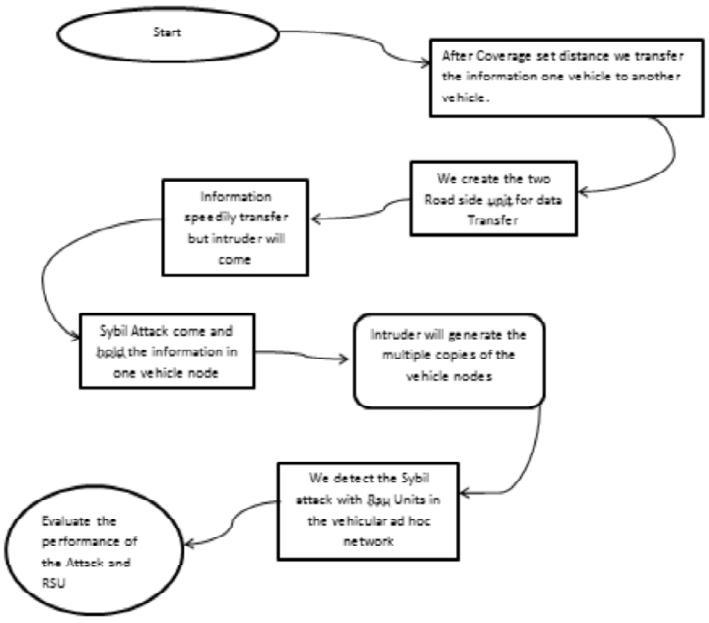


Figure 6: Data Flow Diagram (level 1)

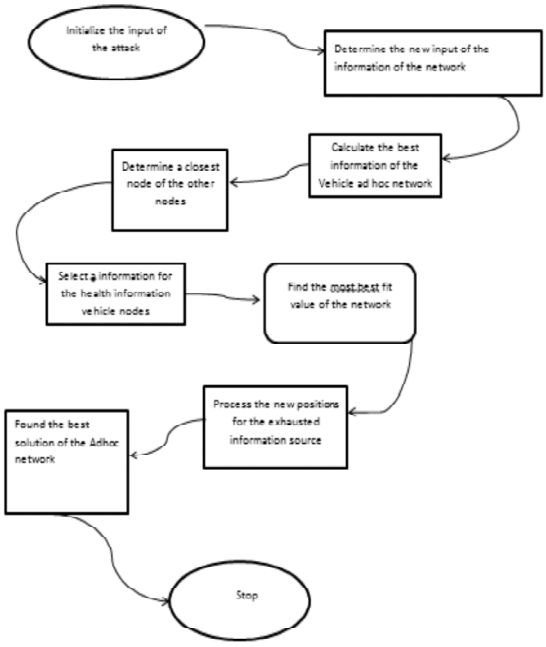


Figure 7:Data Flow Diagram (level 2)

4. IMPLEMENTATION AND WORKING

The subsequent Development Tools has been used in the expansion of this work. There may also be other tools which can be used in this development as it depends person to person and his interest.

Algorithm

Step 1: Initialize N_n
{
// N_n is the network
//N=1 to L,Where L is any real number.

Step 2: for (N=1 , N<α , N++)
{
Initialize l , b

for each l , b = 1 // l,b is the length and Width of the network

Calculate n_n
for n_n =1 , n_n<∞ , n_n ++)
{
Plot (V_n , S_n , D_n)
// Vn is Vehicular node
// Dn is Destination node
// Sn is Source node
}
}
Step 3: function $N_n = f(\alpha)$
Initialize Cs
// C_s is Coverage set
for each C_s = 1
Calculate S , D
Compute d as SÙD
Step 4: function $R_D = f(S)$
Initialize D_{VS}
// Duplicate Vehicular Node
// $D_{VS} = d_n$ (n = 1 to L, Where L is real Number)
Step 5: Apply ABC algorithm for each value of D_{VS}
if $D_{VS} = A_p$
//A_p is achieved performance
end
else
check different value of n

Therefore the used tools are :

- Least amount of 3 GB of RAM
- Intel Pentium III Processor or over
- MATLAB R2010a

Table 1
Tool Used

Computer	*Core 2 Duo or higher*
RAM	3 MB
Platform	Windows 7
Other hardware	Keyboard, mouse
Software	Matlab 2010a

5. RESULTS

- In this section we are describing the result of the vehicular ad-hoc network with road side unit and artificial bee colony optimization techniques. We explained the interface and consequences of the network.

- In the main page figure 8, we design the three buttons first is start means click the start button then open the central page, second button is refresh means refresh the main page and third button click to close the entire figure page**.**

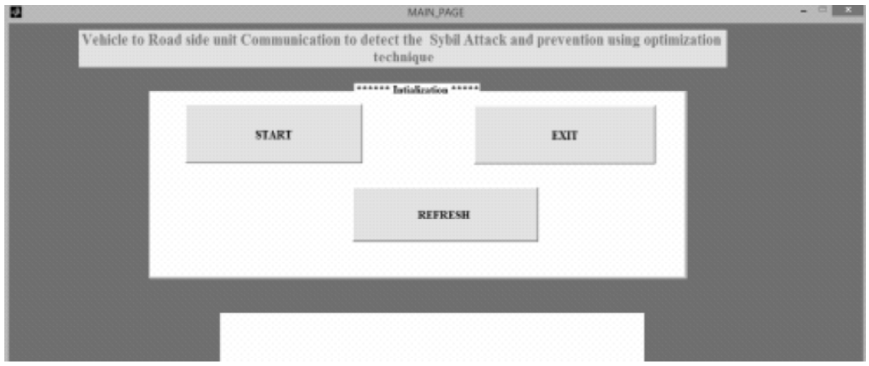


Figure 8: Main Page

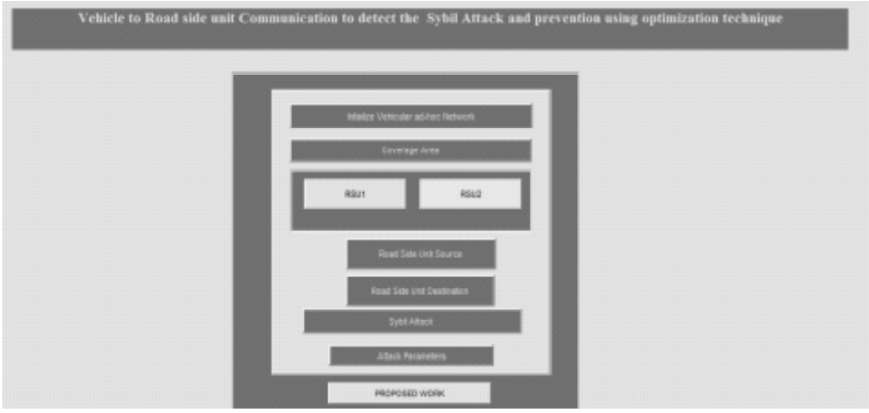


Figure 9: Centre Page

- In figure 9, Initialize the vehicular ad hoc network, create the coverage set and create the trust management in traffic management using road side units. To find the source and destination in road side units. Sybil attack will occur first to detect the attack through road side unit and evaluate the performance with Sybil attack. Sybil attack affect the whole network . Last we apply proposed technique.
- The figure 10, show that the proposed technique using artificial bee colony and evaluate the performance parameters like through put and compare the previous one. The design of vehicular ad hoc network,

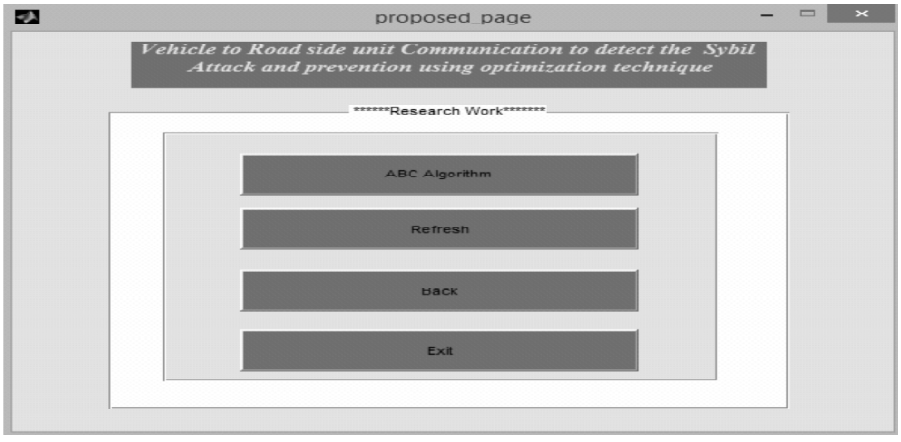


Figure 10: Proposed Technique

display the designed by and qualification. First to initialize the network we need to enter the number of vehicles in ad hoc network. The design the area of the vehicular ad hoc network we create the 1000*1000 area of the network.

- It also shows the coverage set according to the range of the network. The coverage set to find the distance of the range according and calculate the source and destination in the vehicular ad hoc network.
- And Sybil attack defines the multiple copies in the attacker nodes. Since the user doesn't find the original node.
- Here is comparison between Sybil attack and ABC algorithm

A) When number of nodes are 10

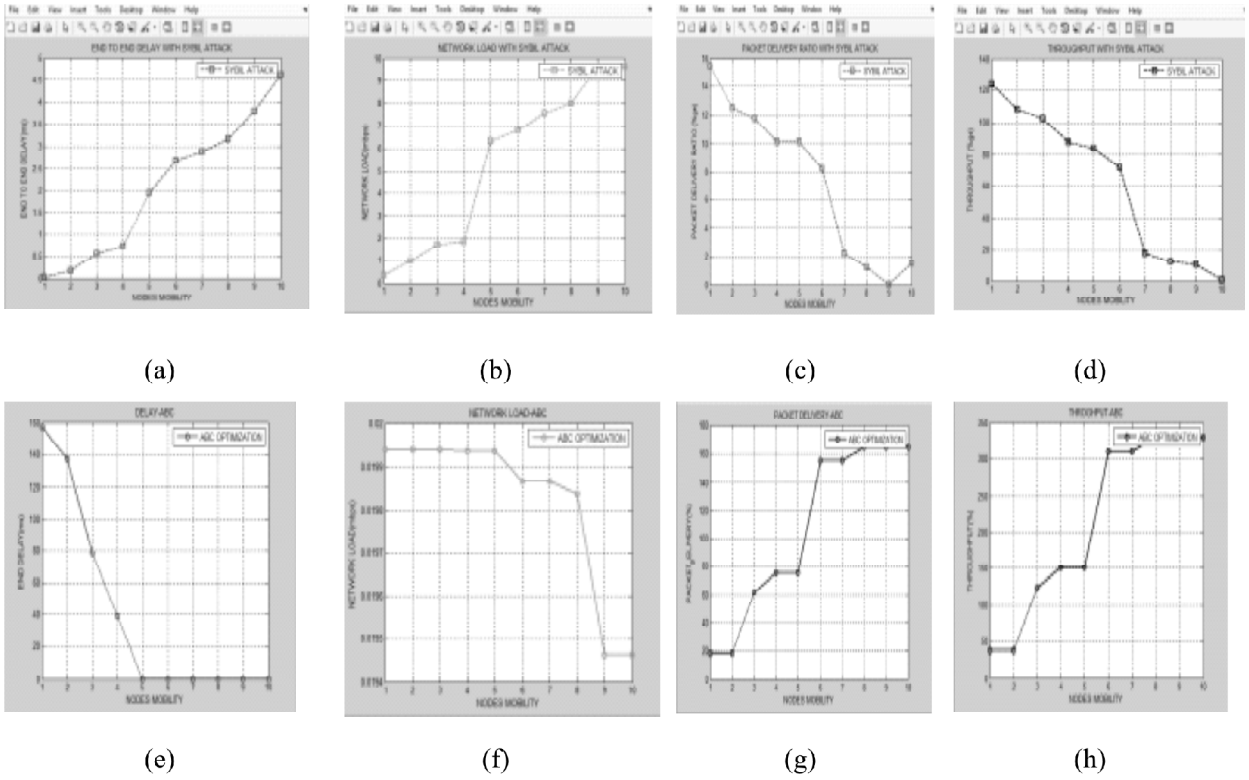
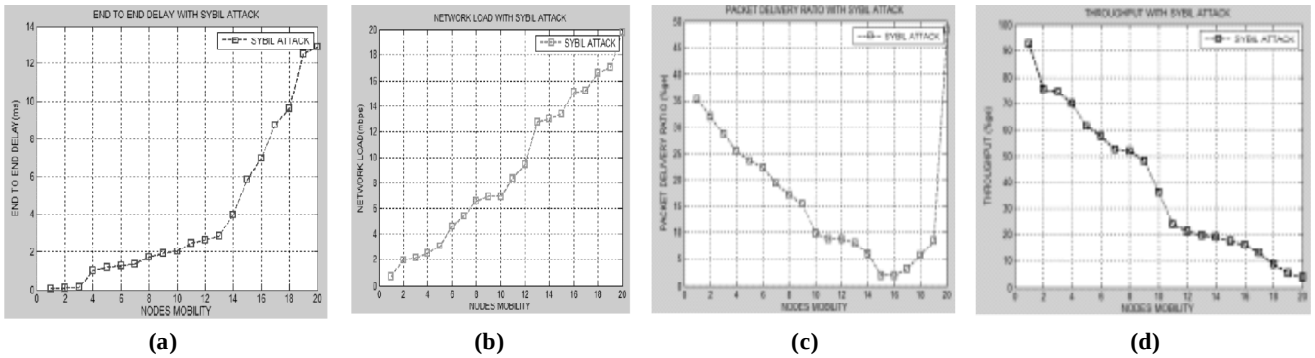
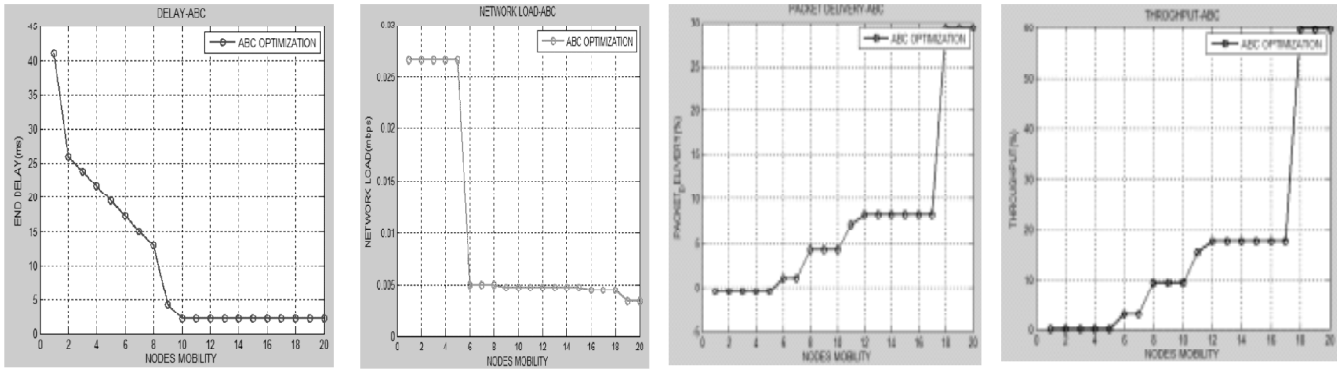


Figure 11: (a)End-to-end delay between 10 nodes with Sybil Attack,(b)Load of the network between 10 nodes with Sybil Attack,(c)Packet delivery rate between 10 nodes with Sybil Attack,(d)Throughput between 10 nodes with Sybil Attack,(e) End-to-end delay between 10 nodes with ABC Algorithm,(f)Load of the network between 10 nodes with ABC Algorithm,(g)Packet delivery rate between 10 nodes with ABC Algorithm ,(h)Throughput by ABC Technique between 10 nodes with ABC Algorithm

B) When number of nodes are 20

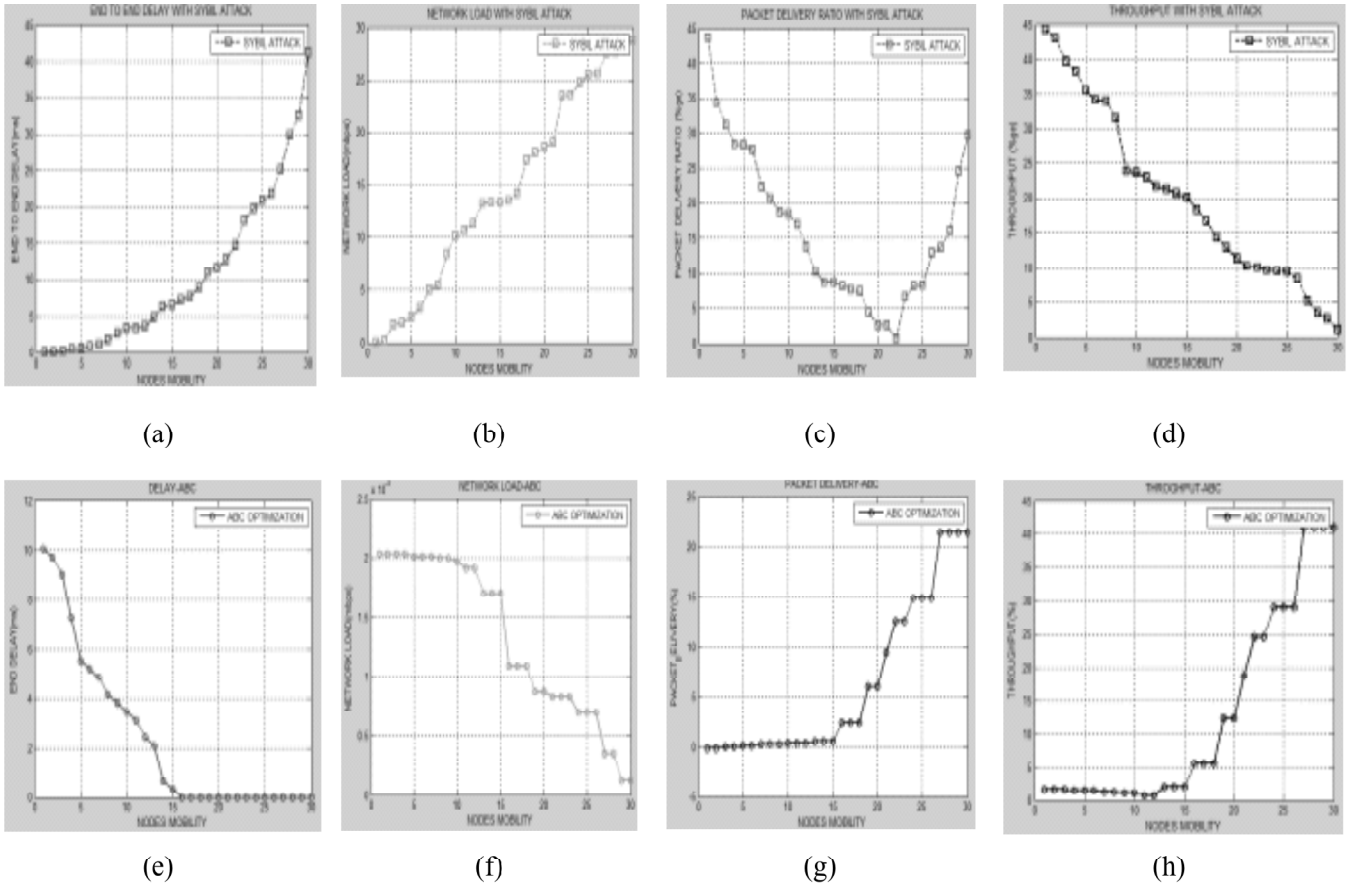




(e) (f) (g) (h)

Figure 12: (a) End-to-end delay between 20 nodes with Sybil Attack,(b)Load of the network between 20 nodes with Sybil Attack, (c) Packet delivery rate between 20 nodes with Sybil Attack, (d)Throughput between 20 nodes with Sybil Attack. (e) End-to-end delay between 20 nodes with ABC Algorithm,(f)Load of the network between 20 nodes with ABC Algorithm, (g) Packet delivery rate between 20 nodes with ABC Algorithm, (h)Throughput between 20 nodes with ABC Algorithm

C) When number of nodes are 30



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 13: (a) End-to-end delay between 30 nodes with Sybil Attack ,(b)Load of the networkbetween 30 nodes with Sybil Attack, (c) Packet delivery rate between 30 nodes with Sybil Attack, (d) Throughput between 30 nodes with Sybil Attack. (e) End-to-end delaybetween 30 nodes with ABC Algorithm, (f) Load of the networkbetween 30 nodes with ABC Algorithm, (g) Packet delivery ratebetween 30 nodes with ABC Algorithm, (h) Throughput between 30 nodes with ABC Algorithm.

- Comparison Between Throughput(Base Paper)

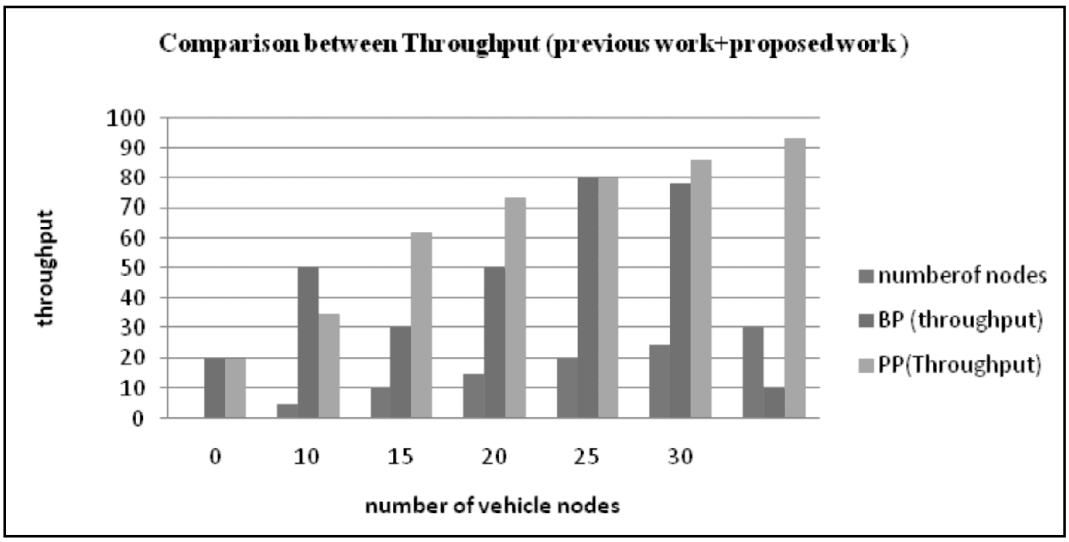


Figure 14: Throughput Comparison

Figure 14 shows comparison of throughput of 30 nodes between previous and proposed work.In this, BP implies Base Paper and PP implies Proposed Paper.

Table 2
Comparison between throughput (Base paper and Proposed Work)

Number of nodes	*BP (throughput)*	*PP (Throughput)*	*Number of nodes*	*BP (throughput)*	*PP (throughput)*
0	20	20	15	50	73.11
5	50	34.51	20	80	80
10	30	62	25	78	86
			30	10	93.56

The above table defines the throughput value with base paper and proposed paper parameters. Throughput means to achieve the maximum accurate network to secure data transmission, but improve the performance with optimization algorithm.

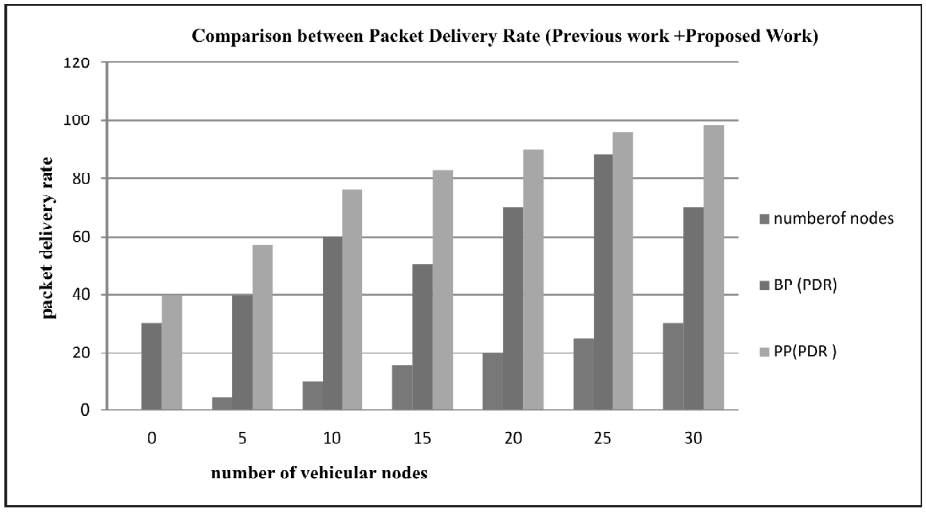


Figure 15: Comparison between Packet Delivery Rate using Base work and Proposed work.

Table 3
Comparison between Packet Delivery Rate (Base paper and Proposed Work)

Numberof nodes	*BP (PDR)*	*PP(PDR)*
0	30	40
5	40	57
10	60	76
15	50	83
20	70	90
25	88	96
30	70	98.56

The above table defines the packet delivery rate value with base paper and proposed paper parameters. Packet delivery rate means to achieve the maximum packet sent the destination of the network to secure data transmission, but improve the performance with optimization algorithm.

6. CONCLUSION

This section defines, plainly identify trials in this environment, review current trust replicas deliberate for different conditions, & judgment out their problems when existence taken to the VANET area. Then we suggest a list of significant belongings that should be archived by trust organization for VANET, situation an exact area for investigators in this area. Our investigation thus attends as single phase faster near the project and expansion of actual trust organization for the positioning of security, life serious and road complaint associated systems by managements and commercial organizations to increase road protection and diminish the amount of car chances and traffic congestion. In this thesis, we have studied an attack on the VANET network known as Sybil Attack which makes false identities from a single entity. Multiple copies are generated through this attack. It causes traffic congestion, jamming etc. This thesis work has formulated our problem and have found a solution to resolve this attack by generating an algorithm called Artificial Bee Colony Algorithm which has been applied in this paper. After that proposed technique have been applied which have improved this thesis results like throughput, packet delivery rate etc.

7. FUTURE SCOPE

In the upgradation, the presence of mischievous leaders who purposefully drop communications. The thesis will examine a set of detection andrevocation apparatuses to cope with this problem by vigorously selecting trustworthy leaders or presenting backup bests and using optimization techniques to mitigate the attack effect in the main network and advance security algorithm applied.

REFERENCES

[1] Samara, Ghassan, and Wafaa AH Ali Alsalihy. “Message Broadcasting Protocols in VANET.” Information Technology Journal 11.9 (2012): 1235.

[2] Shrivastava, Satyam, and Sonali Jain. “A brief introduction of different type of security attacks found in mobile Ad-hoc network.” ACM/Kluwer Wireless Networks Journal (ACM WINET) 9.5 (2003).

[3] Wu, Bing, et al. “A survey of attacks and countermeasures in mobile ad hoc networks.” Wireless Network Security. Springer US, 2007. 103-135.

[4] Grover, Jyoti, M. S. Gaur, and V. Laxmi. “Sybil Attack in VANETs.” Security of Self-Organizing Networks: MANET, WSN, WMN, VANET (2010): 269.

[5] Merlin, Christophe J., and Wendi B. Heinzelman. “A study of safety applications in vehicular networks.” Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on. IEEE, 2005.

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

[7] Kumar, Rakesh, and Mayank Dave. "A comparative study of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).

[8] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks, June 2001, IETF Internet Draft, draft-ietf- manet-brp-01.txt

[9] Festag, Andreas, et al. "Vehicle-to-vehicle and road-side sensor communication for enhanced road safety." Proceedings of the 15th world congress on intelligent transport systems. 2008

[10] 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

[11] Karaboga, Dervis, and Bahriye Akay. "A comparative study of artificial bee colony algorithm." Applied mathematics and computation 214.1 (2009): 108-132.

[12] 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.

[13] 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.

[14] 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.

[15] Rahmat-Samii, Yahya, and Eric Michielssen. "Electromagnetic optimization by genetic algorithms." Microwave Journal 42.11 (1999): 232-232.

[16] Li, Wenjia, and Houbing Song. "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks."IEEE Transaction , 2015.

[17] Alpcan, Tansu, and Sonja Buchegger. "Security games for vehicular networks." Mobile Computing, IEEE Transactions on 10.2 (2011): 280-290.

[18] Luo, Yuyi, Wei Zhang, and Yangqing Hu. "A new cluster based routing protocol for VANET." Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Transaction on. Vol. 1. IEEE, 2010.

[19] 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.

[20] 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.

[21] 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

[22] 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.

[23] 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.

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

[25] 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.

[26] 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.

[27] 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.

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

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