NTBS Protocol in Nibble Bits: A Comprehensive Case Study for VANET Applications

Dr. Ethan Lewis
Department of Biological Sciences, University of Tokyo, Japan

ABSTRACT

The pervasiveness of VANET system network eases our daily activities and improves the communication between world and human beings. The capability of communication among vehicular nodes in VANET environment and transfer of information from one node to another node in every situation under every condition is tremendously increasing day-by-day in Vehicular field. VANET is an emerging technology which provides ubiquitous connectivity among vehicular nodes. VANET system incorporates large number of communicational sensors in order to provide better facilities to passengers in its field reliably and efficiently. Security and privacy issues in VANET system environment had a lot of attention in the research community and addressed at different levels. VANET network security is a more challenging feature than traditional network security because there is a wider range of sensor (device) capabilities, standards, and communication protocols. This paper main objective is to give clear understanding of NTBS Protocol.

Keywords*: VANET, Sensor, MANET, DSRC, Cluster, DGPS, APLM.*

I. INTRODUCTION

Existence of communication among vehicular nodes in order to provide safety conditions on road with best communication is called VANET [1]. Abbreviation for VANET is Vehicular Ad hoc Networks. VANET system environment allows vehicles act as nodes. There are two special kinds of networks available in Ad hoc networks are:

- ***MANET:***

It establishes a transient network without using any infrastructure. The proliferation of mobile devices was tremendously updating and gives importance to communication among mobiles. It is a network which is formed dynamically with collection of nodes to share information in the form of communication [2].

- ***VANET:***

It contains number of efficient sensors for reliable communication. An important design aspect of VANET system is providing best communication among vehicular nodes in its environment. It is a type of network where mobiles behave as nodes. VANET is an emergent technology with excellent features. It contains number of efficient sensors for reliable communication. An important design aspect of VANET system is providing best communication among vehicular nodes in its environment [3**]**.VANET differs from MANET in terms of high mobility and fast dynamic topology. Mobility means to be moved freely and topology means arrangement of nodes in a specific order. In VANET system, each vehicle contains number of device which is used for sending and receiving the data. It is very difficult maintaining route discovery among vehicles in VANET environment because of rapid changing topology. So, properly forming a communication network in VANET depends on the routing of the packet in an effective way. It consists of number of reliable sensors within it for communication.

In VANET, vehicular nodes are connected not only to form a wireless network but also to share information [4]. Each vehicle in this network contains a device which is used for sending and receiving data. VANET aims at providing communication with safe conditions to its users. VANET system environment provides not only sharing of information but also edutainment services, and entertainment services. VANET system allows cars to communicate with each other within a distance of 100-300 meters approximately. Transmission of data or information among vehicles exists through wireless medium in VANET. Main differentiating parameter of VANET from MANET is speed topology of the nodes and speed movement of nodes. Generally the movement of nodes is very fast in VANET comparing with MANET [5].

1.1 VANET Projects

VANET system projects are mostly implemented in Europe. In past years, several numbers of projects on VANET have been undertaken by different countries and different organizations. These all projects main objective was to provide road safety conditions, providing better traffic situations. Every protocol proposed by researchers to test the

feasibility of wireless communication scenario among vehicular nodes. Next place goes to JAPAN and USA. Main VANET projects are,

- C2C-CC
- DEMO
- WAVE
- IVI
- VSC (Vehicle safety communications)
- VII
- SEVECOM
- Coopers
- ASV
- SAFESPOT

By data provided above , it is clear that till now most of the VANET projects implemented in Europe than Japan, USA. So, every country has to implement projects in order to achieve best road safety conditions and to obtain best communication facilities without disconnection in the network of VANET system [6].

1.2 Communication Standards in VANET system

VANET environment uses various communication standards at various countries. To achieve communication means information sharing among vehicular nodes. In VANET environment, the vehicle communicates for safely disseminating the messages. It is challenging task in VANET system because of fast topology change, frequent disruption, and rare contact opportunities. To overcome the problems which are in VANET communication we must implement some communicational standards in VANET environment. We can increase the communication range in VANET environment using different communication standards. For instance, using DSRC communication protocol we increase communication range up to 1000 meters from 300 meters which is normal communication range. It uses different standards country-wise like WAVE; DSRC etc. Now-a-days researchers are focusing on increasing the communication capability of VANET system with security. VANET utilizes DGPS (differential GPS), GPS (Global Positioning System) devices to calculate exact vehicle position. DGPS (Differential GPS) equipped devices to compute exact vehicle position and technologies like Bluetooth detection, sensing method [7].

1.3 DSRC

It was particularly developed for the fulfillment of the requirements of the VANET system. It works on physical and MAC layer of IEEE 802.11 standard [8]. It operates on 75 MHz spectrum in 5.9 GHz frequency band at 27 MBPS data rate in US . In Europe, Japan countries it operates on 30 MHz spectrum in 5.8 GHz band. It provides high level data rate transfers of communication with low latency in small zones. Actually 5.9 GHz band allocated for DSRC by FCC in US to be used by ITS. ITS is the future of transportation. The DSRC spectrum is divided into 7 channels as 1 control channel and 6 service channels operates. The control channel is also used to announce the services that are available. Implementation details are communication range is 300 meters, data rate 6 mbps and broadcast period is 300ns. It means it serves safety applications. Besides, service channels serve non-safety applications. Traffic problems are very big problems in order to transport goods and passengers over the world from one place to other place. The average size of content of a message in VANET system environment is about 100 bytes. The 5.9 GHz DSRC spectrum is divided into seven channels of 10 MHz. The applications of DSRC can be categorized into:

- Routing Based
- Vehicle-to-home
- Vehicle-to-infrastructure
- Vehicle-to-Vehicle

1.4 VANET system Applications

Many applications in VANETs, especially safety related ones; require time sensitive message delivery, often over large distances. Depending different types of communication either V2I or V2V or V2X, the applications of VANET system can be classified as [9].

- Convenience oriented
- Commercial oriented
- Safety oriented
- Productive applications

- Infotainment applications
- Intelligent Transport Applications

This paper organized into six sections. In first section we introduce the main fundamental concepts of VANET system. In second section we explain some related work from previous existing works. In third section, we discuss what is the main method we have to follow in order to get best communication. In section four, we study the possible cases when communication involves with nibble bits. In remaining sections we give acknowledgement and conclusion of this research work. At last we give references which are used in preparing this research work.

II. RELATED WORK

Even though, many protocols were developed, it is clear that no protocol is suitable for getting best communication in VANET system in all situations which provides security. Still researchers are trying to develop protocols to increase the operability in VANET. Gerlach [10] addressed the security concepts for VANET environment and provided appropriate security architecture in VANET communication. This experiment worked good but large storage space. Gowtham [11] achieved communication between nodes take place in secured way by using Random Password Generator and security Wang et al. [12] developed a clustering way on mobility metrics which is based on geographical data. In this, he suggested and proposed stability of a cluster structure and explained the communication overhead for balancing the structure. Fan et al. [13] developed a clustering way by using a cluster creation method. Here, in this method he proposed Dynamic Clustering Algorithm (DCA) to create more stable clusters.

In [14] author et al. discussed attacks which were existed in VANET system. F. Ahammed et al. [15] developed an algorithm called LICA in order to improve the accuracy using GPS devices. Blum et al. [16] proposed a system using Public-Key-Infrastructure to send and receive information of vehicular nodes. Almalag et al. [17] developed an algorithm depends on a clustering technique and similarity of vehicles. Souza et al. [18] developed an algorithm that technique utilizes ALM (Aggregate Local Mobility) technique. The ALM protocol is a beacon depending and aims at increasing the life-time of a cluster.

Azogu [19] proposed an APLM method in order to deliver the content of VANET system environment among vehicular nodes. W. Zhiangang [20] proposed a technique based on heuristic clustering approach. This is also called as PPC (Position-based Prioritized clustering and uses geographic position of vehicular nodes. This MOBIC method calculates signal strength and plays important role in order to increase communication. Venkatamangrao nampally gathers and discussed all clustering methods and invented NTBS protocol by using number theory [21]. In [22] author explained how to achieve fast, reliable and efficient communication mechanism for VANET using TTR method.

III. METHODOLOGY

If we see operations NTBS key generation in table form then next table shows steps occurred inside NTBS clustering protocol NTBS key generation stage are:

Table : NTBS protocol key generation Steps

1.Select a number ‘q’ such that $q \leq 1$ nibble and also Select a number ‘α’ such that $\alpha \leq 1$ nibble	
2. node A chooses a key ‘X_A’’ such that $X_A \leq 1$nibble node B chooses a key ‘ X_B’ such that $X_B \leq 1$nibble and exchange X_A , X_B values	
3. Calculating secure Keys Y_A and Y_B by both nodes and sends to LE	
By node A	By node B
$Y_A=(((q.\alpha)*x_B)*\text{mod}(x_A))$	$Y_B=(((q.\alpha)*x_A)*\text{mod}(x_B))$
4. Exchange Y_A , Y_B values and	

5. Calculating of common NTBS keys by both nodes	
By node A ($NTBS_A$)	By node B ($NTBS_B$)
$NTBS_A$= $(((Y_B)(X_A)\ (Y_A)(X_B))*\mathrm{mod}(Y_B))$	$NTBS_B$= $(((Y_A)(X_B)\ (Y_B)(X_A))*\mathrm{mod}(Y_A))$
6. these values transfer of common NTBS key to LE	
7. LE calculates $NTBS_{final}$ as : $(NTBS_A*Y_B)\ (NTBS_B*Y_A)\ \mathrm{mod}\ (NTBS_A + NTBS_B)$	

IV. RESULT & DISCUSSION

In order to get best results of NTBS Communication Protocol for VANET, we implement this protocol in NAM using NS2 software. Now we limited to discuss only possible nibble bits cases which are gotten during execution of NTBS are :

Case 1:- 1 bit (one digit)

- **NTBS Final Key Generation**

Step 1) First LE selects one number 'q = 7' such that $q \leq 1$ nibble and another number '$\alpha = 5$' such that $\alpha \leq 1$ nibble. Then LE sends that both q, α values to two nodes which want to get authenticated.

Step 2) Now, that two nodes select normal values '$X_A = 2$' (normal key) and '$X_B = 9$' (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

$Y_A = (((q.\alpha)*x_B)*\ \mathrm{mod}(x_A)) = 157$ and

$Y_B = (((q.\alpha)*x_A)*\ \mathrm{mod}(x_B)) = 7$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:

$NTBS_A = (((Y_B)(X_A)\ (Y_A)(X_B))*\mathrm{mod}(Y_B)) = 2826$ (by node A)

And

$NTBS_B = (((Y_A)(X_B)\ (Y_B)(X_A))*\mathrm{mod}(Y_A)) = 126$ (by node B)

Step 6) these common NTBS values transfer to LE.

Step 7) Then LE computes **Final NTBS key** as:

$NTBS_{final} = (NTBS_A* NTBS_B)\ \mathrm{mod}\ (NTBS_A+ NTBS_B) = 120$

- **Node Authentication in NTBS Clustering Protocol**

Example:-

Step 1) LE sends $NTBS_{final}$ = " 120 " key to node A and node B respectively.

Step 2) Node A assumes one number $W_A = 8$ such that $W_A \geq 1$ nibble and sends this number to node B; similarly node B assumes one number $W_B = 5$ such that $W_B \geq 1$ nibble. Both nodes exchange W_A, W_B keys.

Step 3) they calculate preliminary authentication keys [Z_A, Z_B values] as:

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

$= 576000$

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

$= 576000$

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

Step 5) they calculate final authentication value $NTBS_{authent.}$ values as:

$NTBS_{authentA.}$ = $(Z_A * NTBS_{final})$ $(Z_B * NTBS_{final})$ $(W_A * W_B * NTBS_{final})$
= (22923257120000000000)

$NTBS_{authentB.}$ = $(Z_B * NTBS_{final})(Z_A * NTBS_{final})(W_A * W_B * NTBS_{final})$
by node B
= (22923257120000000000)

Case 2:- 2 bits (two digits)

- **NTBS final key generation**

Step 1) First LE selects one number 'q = 97' such that $q \leq 1$ nibble and another number '$\alpha = 76$' such that $\alpha \leq 1$ nibble. Then LE sends that both q, α values to two nodes which want to get authenticated.

Step 2) Now, that two nodes select normal values '$X_A = 53$' (normal key) and '$X_B = 92$' (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
$Y_A = (((q.\alpha)*x_B)* \bmod(x_A)) = 12796$ and
$Y_B = (((q.\alpha)*x_A)* \bmod(x_B)) = 4246$
Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:
$NTBS_A = (((Y_B)(X_A)\ (Y_A)(X_B))*\bmod(Y_B)) = 62393296$ (by node A) and
$NTBS_B = (((Y_A)(X_B)\ (Y_B)(X_A))*\bmod(Y_A)) = 20703496$ (by node B)

Step 6) these common NTBS values transfer to LE.

Step 7) Then LE computes **Final NTBS key** as:
$NTBS_{final} = (NTBS_A * NTBS_B) \bmod (NTBS_A + NTBS_B) = 15545237$

- **Node authentication in NTBS clustering protocol**

Example:-

Step 1) LE sends $NTBS_{final}$ = " 15545237 " key to node A and node B respectively.

Step 2) Node A assumes one number $W_A = 48$ such that $W_A \geq 1$ nibble and sends this number to node B; similarly node B assumes one number $W_B = 91$ such that $W_B \geq 1$ nibble. Both nodes exchange W_A, W_B keys.

Step 3) they calculate preliminary authentication keys [Z_A, Z_B values] as:
$Z_A = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$
$= 1055546390310786192$
$Z_B = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$
$= 1055546390310786192$

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

Step 5) they calculate final authentication value $NTBS_{authent.}$ values as:
$NTBS_{authentA.}$ = $(Z_A * NTBS_{final})$ $(Z_B * NTBS_{final})$ $(W_A * W_B * NTBS_{final})$
=8282236485233254967765504096781836004399821811469957577363456

$NTBS_{authentB.}$ = $(Z_B * NTBS_{final})(Z_A * NTBS_{final})(W_A * W_B * NTBS_{final})$
by node B
=8282236485233254967765504096781836004399821811469957577363456

Case 3:- 3 bits (three digits)

- **NTBS final key generation**

Step 1) First LE selects one number 'q = 973' such that q ≤ 1 nibble and another number 'α = 854' such that α ≤ 1 nibble. Then LE sends that both q, α values to two nodes which want to get authenticated.

Step 2) Now, that two nodes select normal values 'X_A = 623' (normal key) and 'X_B = 754' (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
$Y_A = (((q.\alpha)*x_B)* \bmod(x_A)) = 1005666$ and
$Y_B = (((q.\alpha)*x_A)* \bmod(x_B)) = 686574$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:
$NTBS_A = (((Y_B)(X_A)\ (Y_A)(X_B))*\bmod(Y_B)) = 472403558172$ (by node A)
and
$NTBS_B = (((Y_A)(X_B)\ (Y_B)(X_A))*\bmod(Y_A)) = 322512643908$ (by node B)

Step 6) these common NTBS values transfer to LE.

Step 7) Then LE computes **Final NTBS key** as:
$NTBS_{final} = (NTBS_A * NTBS_B) \bmod (NTBS_A + NTBS_B) = 191663121394$

- **Node authentication in NTBS clustering protocol**

Example:-
Step 1) LE sends $NTBS_{final}$ = " 191663121394 " key to node A and node B respectively.

Step 2) Node A assumes one number W_A = 935 such that $W_A \geq 1$ nibble and sends this number to node B; similarly node B assumes one number W_B = 896 such that $W_B \geq 1$ nibble. Both nodes exchange W_A, W_B keys.

Step 3) they calculate preliminary authentication keys [Z_A, Z_B values] as:
$Z_A = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$
$= 307749059213830113 78390991360$
$Z_B = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$
$= 307749059213830113 78390991360$

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

Step 5) they calculate final authentication value $NTBS_{authent.}$ values as:
$NTBS_{authentA.} = (Z_A * NTBS_{final})\ (Z_B * NTBS_{final})\ (W_A * W_B * NTBS_{final})$
=55863579324511152473238729450697186591706615115239508275729081560222058475233592626903661936 64000

$NTBS_{authentB.} = (Z_B * NTBS_{final})(Z_A * NTBS_{final})(W_A * W_B * NTBS_{final})$ by node B

=55863579324511152473238729450697186591706615115239508275729081560222058475233592626903661936 64000

Case 4:- 4 bits (nibble)

- **NTBS final key generation**

Step 1) First LE selects one number 'q = 1234' such that q ≤ 1 nibble and another number 'α = 5678' such that α ≤ 1 nibble. Then LE sends that both q, α values to two nodes which want to get authenticated.

Step 2) Now, that two nodes select normal values 'X_A = 2345' (normal key) and 'X_B = 8765' (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

$Y_A = (((q.\alpha)*x_B)* \mod(x_A)) = 26189042$ and
$Y_B = (((q.\alpha)*x_A)* \mod(x_B)) = 1874569$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:
$NTBS_A = (((Y_B)(X_A)\ (Y_A)(X_B))*\mod(Y_B)) = 538287605089850$ (by node A)
And
$NTBS_B = (((Y_A)(X_B)\ (Y_B)(X_A))*\mod(Y_A)) = 38529750633325$ (by node B)

Step 6) these common NTBS values transfer to LE.

Step 7) Then LE computes **Final NTBS key** as:
$NTBS_{final} = (NTBS_A * NTBS_B) \mod (NTBS_A + NTBS_B) = 35956073421402$

- **Node authentication in NTBS clustering protocol**

Example:-
Step 1) LE sends $NTBS_{final}$ = " 35956073421402 " key to node A and node B respectively.

Step 2) Node A assumes one number $W_A = 6214$ such that $W_A \geq 1$ nibble and sends this number to node B; similarly node B assumes one number $W_B = 8376$ such that $W_B \geq 1$ nibble. Both nodes exchange W_A, W_B keys.

Step 3) they calculate preliminary authentication keys [Z_A, Z_B values] as:
$Z_A = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$
$= 67290295385791731786402000440552256$
$Z_B = (NTBS_{final} * W_A)\ (NTBS_{final} * W_B)$
$= 67290295385791731786402000440552256$

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

Step 5) they calculate final authentication value $NTBS_{authent.}$ values as:
$NTBS_{authentA.} = (Z_A * NTBS_{final})\ (Z_B * NTBS_{final})\ (W_A * W_B *.NTBS_{final})$
=1095543339359398153414785356925247737122501126049127631869678456419581313234569287718228540679792611569709775034200883 2

$NTBS_{authentB.} = (Z_B * NTBS_{final})(Z_A * NTBS_{final})(W_A * W_B * NTBS_{final})$
by node B

=1095543339359398153414785356925247737122501126049127631869678456419581313234569287718228540679792611569709775034200883 2

V. CONCLUSION

Communication in VANET system is rapidly increasing; rising technology that has attaining a considerable amount of the attention in the view of both passengers and drivers. This paper gives clear picture about NTBS Protocol results in NAM used with NS2 software. And also here, we provided important cases which are arisen. it is clear that **security is directly proportional to the number of bits used in keys of network.**

VI. ACKNOWLEDGEMENTS

The author would like to express his heartfelt thanks to research persons who contributed in this research work either directly or indirectly.

REFERENCES

1. *Venkatamangarao Nampally, Dr. M. Raghavender Sharma , "Increasing Information Sharability by Using NTBS Clustering Approach for VANET", IPASJ International Journal of Computer Science (IIJCS), Vol.**5,** Issue.**10**, pp.**1-17**, **2017.***
2. *Chlamtac. I., Conti. M., and Liu. J. J.-N," Mobile Ad hoc Networking: Imperatives and Challenges: Ad Hoc Networks", vol. **1**, pp. **13–6**, **2003.***
3. *Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie,"Vehicular Ad Hoc Networks:Architectures,Research Issues, Methodologies, Challenges and Trends", International Journal of Distributed Sensor Networks, Article ID **745303**, **2015.***
4. *Venkatamangarao Nampally, Dr. M. Raghavender Sharma, "Reliable and Efficient Routing Mechanisms for VANET", Asian Journal of Computer Science and Technology (AJCST), Vol. **7,** No. **2**, **2018.***
5. *http://ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part4-13VehicleToVehicle-HR.pdf*
6. *Hannes Hartenstein et al., and Kenneth P. Laberteaux,"A Tutorial Survey on Vehicular Ad Hoc Networks" , IEEE Communication Magazine, pp. **164-171**, **2008.***
7. *Elmar Schoch, Frank Kargl, and Michael Weber, "Communication Patterns in VANETs", IEEE Communications Magazine, pp. **119- 125**, **2008.***
8. *Qing Xu, Tony Mak, jeff Ko, and Raja Sengupta, "Vehicle-to-Vehicle Saftey Messaging in DSRC", in the proceeding of ACM VANET, **Philadelphia**, **2004.***
9. *S. S. Manvi, M. S. Kakkasageri, D. G. Adiga, " Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach", in International Conference on Future Computer and Communication, pp. **16-20**, **2009.***
10. *Gerlach, VaneSe , " An Approach to VANET Security", in the proceedings of V2VCOM, **2005**.*
11. *G.Gowtham , E.Samlinson, "A Secured Trust Creation in VANET Environment Using Random Password Generator," International Conference on Computing, Electronics and Electrical Technologies [ICCEET]. PP: **781-784**, **2012.***
12. *Z. Wang, L. Liu, M. Zhou, and N. Ansari," A position based clustering technique for ad hoc intervehicle communication", IEEE Trans. Syst. Man Cybern., Part C, Appl. Rev., vol. **38**, no. **2**,pp. **201–208**, **2008.***
13. *W. Fan, Y. Shi, S. Chen, L. Zou, "A mobility metric based dynamic clustering algorithm (DCA) for VANETs", in the International Conference on Communication Technology and Application, **Beijing**, pp.**752–756**, **2011.***
14. *Venkatamangarao Nampally, Dr. M. Raghavender Sharma, "Traditional Data Encryption Methods for VANET", International Journal of Advance Scientific Research and Engineering Trends (IJASRET), Vol.**2**, Issue.**4,** pp.**32-35**, **2017.***
15. *F. Ahammed, J. Taheri, and A. Zomaya, " LICA: Robust Localization Using Cluster Analysis to Improve GPS Coordinates", in the ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, New York, **USA**, pp.**39–46**, **2011.***
16. *J. Blum, A. Eskandarian, and L. Hoffman," The Challenges of Inter Vehicle Ad Hoc Networks", IEEE Transactions of Intelligent Transportation Systems, Vol. **5**, No. **4**, pp. **347-351**, **2004.***
17. *S. Almalag Mohammad, and C. Weigle Michele," Using Traffic Flow For Cluster Formation in Vehicular Ad hoc Networks", In IEEE Local Computer Networks (LCN) Conference , IEEE, Denver, CO, **USA**, pp. **631-636**, **2010.***
18. *E. Souza,I. Nikolaidis, and P. Gburzynski," A new aggregate local mobility (ALM) clustering algorithm for VANETs", In international conference on Communications (ICC), IEEE, Cape town, **South Africa**, pp. **1-5**, **2010.***
19. *Azogu, I.K., Ferreira, M.T., and Hong Liu, "A security metric for VANET content delivery", Global Communications Conference (GLOBECOM),IEEE , pp.**991-996**, **2012.***
20. *W. Zhiangang, L. Lichuan, Z. MenhChu, and A. Nirwan, "" A Position based Clustering Technique for Ad hoc Intervehicle Communication", IEEE Trans. Syst. Man Cybern., Part C, Appl. Rev., vol. **38**, no. **2**, pp. **201–208**, **2008.***
21. *Venkatamangarao Nampally, Dr. M. Raghavender Sharma , "Increasing Information Sharability by Using NTBS Clustering Approach for VANET", IPASJ International Journal of Computer Science (IIJCS), Vol.**5,** Issue.**10**, pp.**1-17**, **2017.***
22. *Venkatamangarao Nampally, Dr. M. Raghavender Sharma, "Achieving Fast Communication Mechanism by Using Transitive Trust Relationships for VANET", International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), Vol.**2**, Issue.**5**, pp.**349-355**, **2017.***