International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

A Theoretical Research on NTBS Protocol : Its Implementation and Possibilities in Nibble-bits in NAM for VANET Security

Venkatamangarao Nampally
Research Scholar, Department of Computer Science
University College of Science, Osmania University
Hyderabad, India.

Dr. M. Raghavender Sharma
Asst. Professor, Department of statistics
University College of Science, Osmania University
Hyderabad, India

***Abstract*—The tremendous development of wireless communication technology has revolutionized human lifestyles in providing the most convenience and flexibility over accessing internet services and reliable services offered for privacy and security. Research on VANETs has been receiving increasing interest both in the algorithmic aspects as well as standardization efforts due to the high mobility and sparse distribution of the vehicles on the road. VANET environment is the promising approach to provide traffic, safety and other applications to the drivers as well as passengers. In VANET, achievements are meant for not only reliable data delivery but also the delivery of information efficiently with security. Security is an important aspiration for VANET in view of the facts that improved security which reduces accidents and consequently improves traffic conditions and yet save lives. Clustering algorithms have emerged as an alternative powerful learning tool accurately analysis the massive volume of data generated by using modern technology in order to deliver a message to its destination. Clustering is using to improve routing scalability and reliability in VANET system, as it results in the distributed formation of hierarchical network structures by grouping vehicles together based on correlated spatial distribution and relative velocity. Depends on the IEEE 802.11p standard, the dedicated short range communication (DSRC) system supports two types of communication environments: First is vehicle-to-infrastructure (V2I) and second is vehicle-to-vehicle (V2V) communication. In this article, we can increase the information shareability by using NTBS clustering protocol by using TTRs concept.**

Keywords—VANET; NTBS; Nibble-bits; Ad-Hoc Network; Wireless Communication; DSRC;

I. INTRODUCTION

An Ad hoc Network itself is a system of network forming arbitrary topology with P2P connection. It is called as decentralized network. If network will create for short period of time then it is termed as Ad hoc network. In Ad hoc networks the goal will be increasing the mobility and flexibility [1, 2, and 3].

Existence of communication among vehicular nodes in order to provide safety conditions on road with best communication is called VANET. Very high number of people is sharing of information in VANET system. So, providing security to information sharing is must. In VANET system, each vehicle contains number of device which is used for sending and receiving the data [4].

In VANET system every node should maintain connectivity with other vehicular nodes in order to obtain best communication facility. Without security, information sharing is meaningless and an attacker easily attack on that information and also assets of network are damaged by corrupting the whole network [5]. We can provide security using secure protocols. In secure protocols, increase of communication range directly proportional to secure protocol involved. The goal of our paper is to increase the communication capability in VANET system environment **to** achieve the secure communication by developing NTBS Clustering protocol for VANET in ubiquitous Computing Environment.

The usage of automobiles provides many benefits to society, including transportation provision, and revenue generation from the tax opportunities and travel facilities. Vehicles play an important role in our daily life in providing transportation facility to carry goods from one place to another place, and comfort with safety conditions to passengers as well as drivers. Messages exchanged in VANETs to increase the range of awareness of drivers beyond their authentication level, thus significantly improving safety and comfort conditions to all passengers in a vehicular node [6]. VANET system environment provides, a plethora of other applications such as collision avoidance, and entertainment of passengers including chatting, interactive games, file sharing etc. VANET system allows vehicular nodes to communicate with each other within a distance of 100-300 meters approximately. Hence, 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. The large number of exchanged messages between vehicles in dense traffic can cause overloading of the available network resources and thus congestion related delays. On the other hand, low traffic densities often cause the network to be intermittently connected [7].

A modern vehicle is a network of Sensor parts on wheels. Normally a modern vehicle contains Forward/backward radar, GPS, Computing platform, human-machine interface, EDR and TPD. 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 [8].

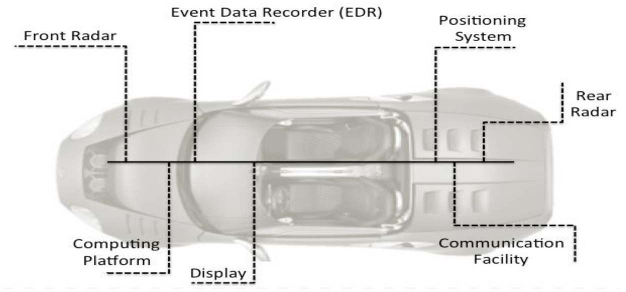


Fig. 1. A Modern Vehicle Overview

A. The Major Components of a VANET system

The Wireless On-Board Unit (OBU):- it is used to authenticate nodes (vehicles) with another node in specified network.

The Roadside Unit (RSU):- it is used to give signals to nodes which are moving to get authentication.

And the **Authentication Server (AS):-** it will be stored all key pairs.

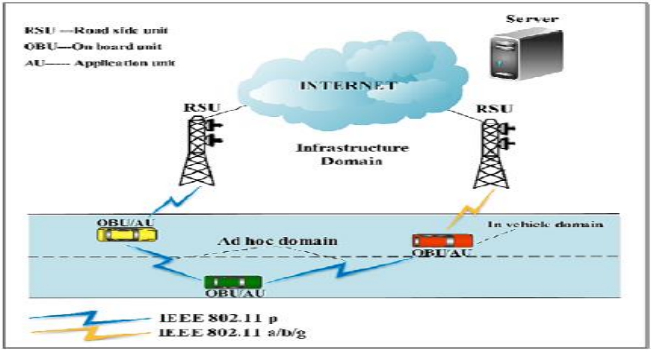


Fig. 2. Main components of VANET system

In getting communication inside VANET system environment, vehicular nodes role is very important. In VANET system environment all vehicles communicate by using some wireless system technologies such as DSRC IEEE 802.11p, MBWA, and IEEE 802.20.

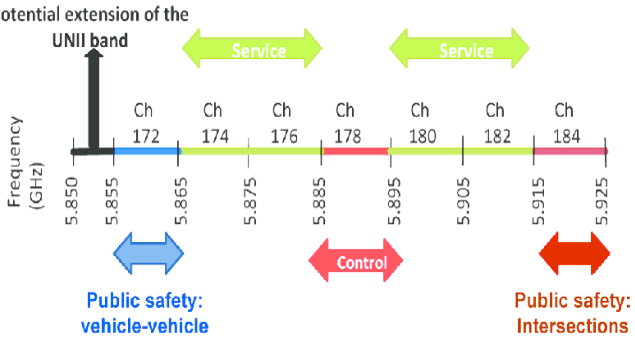


Fig. 3. DSRC channels for VANET system

TABLE I. STANDARDS OF DSRC IN, USA, JAPAN, AND EUROPE

Features	**USA Standards**	**Japan Standards**	**Europe Standards**
Data Rate Use	3-27 MBPS in both links	1 MBPS for downlink 4 MBPS for uplink	500 KBPS for downlink 250 KBPS for uplink
Spectrum Band	75 MHz	80 MHz	20 MHz
Channels	7	7	4
Transmission Range	1000 m	30 m	15-20 m
Communication model	Half duplex	Half-duplex in OBU Full-duplex in RSU	Half-duplex
Radio frequency	5.9 GHz	5.8 GHz	5.8 GHz
Channel Separation	10 MHz	5 MHz	5 MHz

DSRC 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. 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 [9]. It provides high level data rate transfers of communication with low latency in small zones. 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.

B. Major Problem in VANET System

The problem inside VANET system was achieving communication without providing security among vehicles. To overcome this big problem I proposed NTBS (Network Theory Based Secure) Clustering protocol to increase information shareability with TTRs Concept in VANET system environment. It can increase the capability of sharing of information. For the review, we have discussed the taxonomy of clustering approaches and grouping them into six groups and review these protocols. 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.

C. Flow of Communication in VANET System

To share information among vehicles in VANET environment, communication is must. Communiation can be obtained in VANET system using communication components. In VANET environment communication can be achieved using some standard protocols mainly in four ways. These are [10]:

V2I, V2V, V2C, and V2B.

II. LITERATURE SURVEY

Still researchers are trying to develop protocols to increase the communication capability in VANET [11]. Here, authors addressed the security concepts for VANET environment and provided appropriate security architecture in VANET communication. This experiment worked good but large storage space. [12] achieved communication between nodes take place in secured way by using Random Password Generator and security algorithms similar to ECDSA [13] and TESLA [14]. Clustering has been widely used to disseminate the message to their end point [15]. To achieve fast communication with security is one of the major problems in VANET. ECC [16] method by Menezes, S. Vnstone, and D. Hankerson achieved best security but with high computation cost. Wang et al. [17] 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. [18] 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. F. Ahammed et al. [19] developed an algorithm called LICA in order to improve the accuracy using GPS devices. Blum et al. [20] proposed a system using Public-Key-Infrastructure to send and receive information of vehicular nodes. Sivagurunathan et al. [21] developed a method which was self-key managed using clustering technique by dividing the network is into sub- clusters. Almalag et al. [22] developed an algorithm depends on a clustering technique and similarity of vehicles. Souza et al. [23] 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. Kayis et al. [24] developed clustering way classified vehicles on speed range to form clusters for achieving communication among vehicular nodes. Sun [25] proposed a security method based on identity of a vehicle to preserve user privacy in VANET environment. Azogu [26] proposed an APLM method in order to deliver the content of VANET system environment among vehicular nodes. Kamlesh Namdev [27] proposed a clustering algorithm to provide efficient and secure communication in VANET system. W. Zhiangang [28] 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. Little [29] proposed a clustering method DPP (direction Propagation method) which is based on MOBIC technique in VANET system. This MOBIC method calculates signal strength and plays important role in order to increase communication.

III. PROPOSED WORK

A. *Significance of Proposed Work*

Study of set of positive whole numbers is called Number theory. It is concerned with properties of integers. It plays an important role to provide security feature to a communication. Modular-arithmetic-based concept is the central mathematical concept in number theory. Modular arithmetic approach was developed by **Carl Friedrich Gauss.** “Modulus” (abbreviated as “mod”) is the word for “residue or remainder”. Security measures guarantees the transmissions of data and make that data accessible only by authorized parties. In order to achieve general authentication and to make it secure communication among nodes in a cluster of VANET system (Venkatamangarao Nampally, Dr. M. Raghavender Sharma, 2017), we have proposed Number Theory Based Security (NTBS) clustering protocol method. It gives not only communication but also provides security to communication. If the authentication procedure done successfully, the vehicle is trustful vehicle (TV), otherwise it is considered as mistrustful vehicle (MV).The MV requires to obtain the authentication successfully in order to change from MV into TV. The trustful vehicles change the MVs into TVs performing the authentication procedure.

The proposed NTBS clustering scheme provides security feature to shareable information in VANET system environment. This scheme involves with the following procedures:

TABLE II. PROPOSED SYSTEM PROCEDURES

1.LE Registration,
2. NTBS clustering Protocol key generation.
3. Node Authentication
4. Transitive Trust Relationships

This final NTBS key sends to all nodes which are inside a cluster. 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. Similarly by using TTR concept (Venkatamangarao Nampally, Dr. M. Raghavender Sharma, 2017) communication will be flown in total cluster.

B. *Details of Proposed Implementation*

In order to implement NTBS Clustering protocol in VANET communication, we have used some simulation tools and parameters. A Simulator can predict the behavior of a network. Computer simulation can be used to assist the modeling and analysis in many natural systems. NS2 simulator abbreviation is Network Simulator version 2. It is developed primarily for UNIX based OS. Now it supports all OS platforms including MS-windows, Solaris and Linux mint. It is mainly used to predict the behavior of MANETs as well as VANETs. It is licensed for use under GNU (Kevin Fall, and Kannan Vardhan, 2000). The primary use of NS is in network research to simulate various types of wired/wireless local and wide area networks.

To implement this ns2 project we should use following software and packages are:

- NS 2.35 installation folder
- TCL binary files folder
- WINRAR (to extract)
- Cygwin Terminal/ XWin Server
- Notepad++
- ActiveTcl8.6.1.0.
- NAM
- XGraph

A network simulator predicts the behavior of a computer network environment and gives accurate understanding of system behavior with packet level communication flow in network. NS2 is one of the most popular simulators used in network research that focuses on the simulation of IP networks on the packet level. It is open source and freely available software and developed at the University of Berkeley. This project started with LBL, Xerox PARC, UCB, and USC/ISC. It is available for platforms FreeBSD, Linux, SunOS/Solaris, MAC OSX and all windows versions. TCL scripting language is used for specifying scenarios, traffic patterns and events. We carefully analysis the trace files for calculating the performance of network protocols. NS2 are discrete simulation events aimed in networks researches. It provides support for simulation of TCP. NS2 can be run on multitasking, multiuser computer operating systems and windows (XP, VESTA and 7). It uses Terminal Command Language (TCL) as its scripting language (Venkatamangarao Nampally, Dr. M. Raghavender Sharma, 2017). The TCL language is used to design the network (set parameters, node configurations, and topology, connection between nodes, transfer packages and simulation time). Furthermore, C++ language is used for the security package (encryption /decryption). NS2 combines both languages strengths and uses both languages in order to get excellent simulation scenario. In NS2 readymade compiled C++ objects available. C++ for data implementation and back-end supports (internal mechanism). It is used to run simulation. It also helpful in reducing processing time of packets and thus decreases the packet loss ratio in VANET system environment. It is fast to run but slower in modify code and change. OTCL for code controlling, co-ordination, and set-up simulation. It is easy to create or edit code but runs slowly.

C. Proposed System Steps

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’ 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’ (normal key) and ‘X_B’ (normal key) respectively such that $X_A \leq 1$ nibble, and $X_B \leq 1$ nibble. Then nodes exchange X_A and X_B values between them.

Step 3) And compute their Secure keys Y_A, Y_B as $Y_A = (((q.\alpha)_* x_B)_* \bmod(x_A))$ and
$Y_B = (((q.\alpha)_* x_A)_* \bmod(x_B))$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:

$NTBS_A = (((Y_B)(X_A)\ (Y_A)(X_B))_* mod(Y_B))$ (by node A)

and

$NTBS_B = (((Y_A)(X_B)\ (Y_B)(X_A))_* mod(Y_A))$ (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 $(NTBS_A + NTBS_B)$

This $NTBS_{final}$ value sends to node A, B to get these nodes to be authenticated.

IV. SIMULATION RESULTS

A. NTBS Protocol Possibilities in Nibble-bits

In computer memory terminology, 1 nibble = 4 bits. So, we can take four types of values in NTBS clustering protocol. Every time we change value in terms of bits then trace files get affected. Now let’s we examine each case with example.

1) Case 1: 1 bit(one digit)

Example:

Step 1) First LE selects one number ‘q = 7’ such that q ≤ 1 nibble and another number ‘α = 5’ 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 ‘$X_A = 2$’ (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

$Y_A = (((q.\alpha)_* x_B)_* \bmod(x_A)) = 157$ and $Y_B = (((q.\alpha)_* x_A)_* \bmod(x_B)) = 7$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:

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

and

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

Step 6) these common NTBS values transfer to LE.

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

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

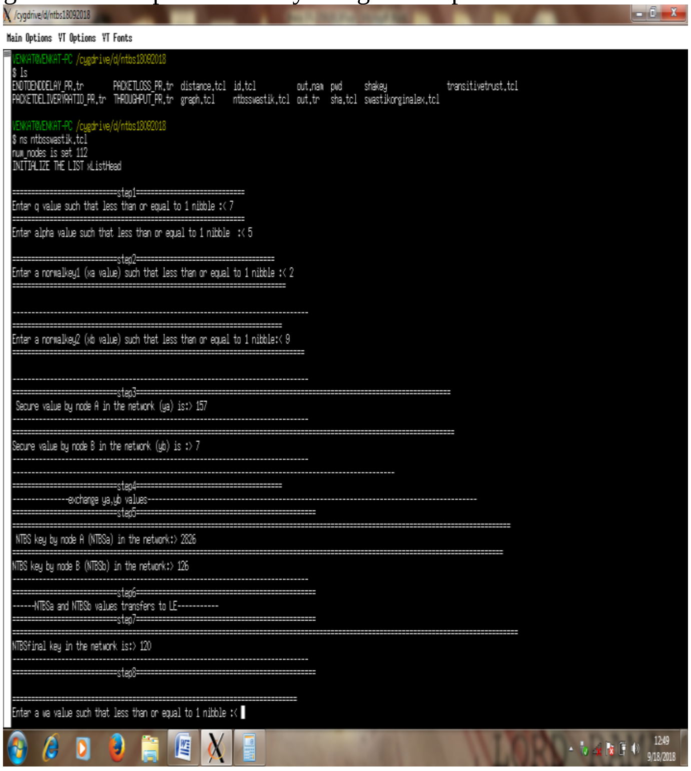
If we see operations NTBS key generation example in table form then it shows steps occurred inside NTBS clustering protocol NTBS key generation stage are:.

TABLE III. NTBS PROTOCOL KEY GENERATION STEPS WHEN VALUES ARE ≤ 1NIBBLE

1.Select a number ‘q = 7 ’ such that q ≤ 1 nibble and also Select a number ‘α = 5’ such that α ≤ 1 nibble	
2. node A chooses a key ‘$X_A = 2$’ such that $X_A \leq 1$ nibble node B chooses a key ‘ $X_B = 9$’ 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
$Y_A=(((q.\alpha)_* x_B)_* mod(x_A)) =$ 157	$Y_B=(((q.\alpha)_* x_A)_* mod(x_B))=$ 7
4. Exchange Y_A , Y_B values and	

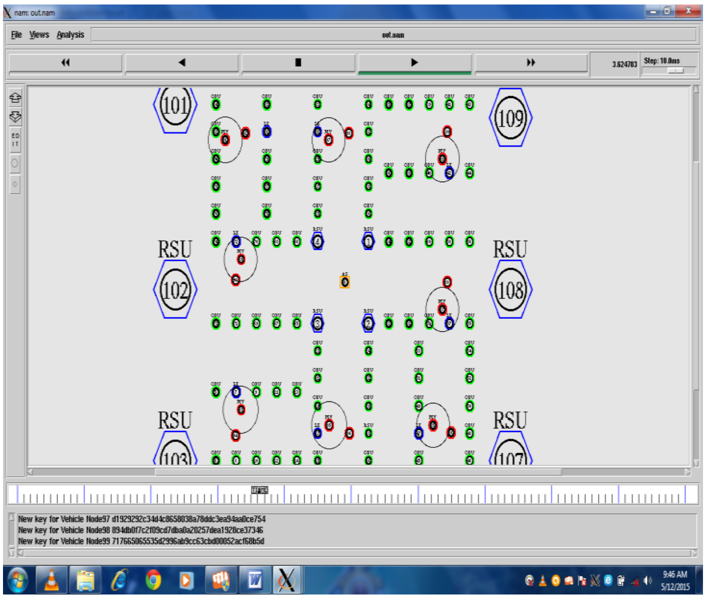
5. Calculating of common NTBS keys by both nodes	
By node A ($NTBS_A$)	By node B ($NTBS_B$)
$NTBS_A$= $(((Y_B)(X_A)\ (Y_A)(X_B))_*\mathrm{mod}(Y_B))$ = 2826	$NTBS_B$= $(((Y_A)(X_B)(Y_B)(X_A))_*\mathrm{mod}(Y_A))$ = 126
6. these values transfer of common NTBS key to LE	
7. LE calculates $NTBS_{final}$ as : $(NTBS_A{*}Y_B)\ (NTBS_B{*}Y_A)$ mod $(NTBS_A + NTBS_B)$ = 120	

a) Key generation steps in NAM: Now lets discuss key generation steps in NAM by using NTBS protocol.



```
VENKAT@VENKAT-PC /cygdrive/d/ntbs18092018
$ ls
ENDTOENDDELAY_PR.tr       PACKETLOSS_PR.tr  distance.tcl  id.tcl          out.nam  pwd     shakey                transitivetrust.tcl
PACKETDELIVERYRATIO_PR.tr THROUGHPUT_PR.tr  graph.tcl     ntbsswastik.tcl out.tr   sha.tcl swastikorginalex.tcl

VENKAT@VENKAT-PC /cygdrive/d/ntbs18092018
$ ns ntbsswastik.tcl
num_nodes is set 112
INITIALIZE THE LIST xListHead

========================step1========================
Enter q value such that less than or equal to 1 nibble :< 7
=====================================================
Enter alpha value such that less than or equal to 1 nibble  :< 5

========================step2===============================
Enter a normalkey1 (xa value) such that less than or equal to 1 nibble :< 2
==============================================================


-------------------------------------------------------------------
=============================================================
Enter a normalkey2 (xb value) such that less than or equal to 1 nibble:< 9
==================================================================


-------------------------------------------------------------------
========================step3====================================================================
 Secure value by node A in the network (ya) is:> 157
-------------------------------------------------------------------
====================================================================================================
Secure value by node B in the network (yb) is :> 7
-------------------------------------------------------------------
-------------------------------------------------------------------------------------
========================step4==============================
-------------exchange ya,yb values-----------------------------------------------------------------------------
========================step5=====================================
================================================================================================================
 NTBS key by node A (NTBSa) in the network:> 2826
==============================================================================================================
NTBS key by node B (NTBSb) in the network:> 126
-------------------------------------------------------------------
========================step6=====================================
------NTBSa and NTBSb values transfers to LE-----------
========================step7=====================================
=================================================================================================================
NTBSfinal key in the network is:> 120
-------------------------------------------------------------------
========================step8=====================================

================================================================
Enter a wa value such that less than or equal to 1 nibble :<
```

*b) Final Communication in NAM :*After generating all keys and if we enguage that keys in Nam then final communication would be as follows.



```
New key for Vehicle Node97 d1929292c34d4c8658038a78ddc3ea94aa0ce754
New key for Vehicle Node98 894db0f7c2f09cd7dba0a20257dea1928ce37346
New key for Vehicle Node99 717665065535d2996ab9cc63cbd00052acf68b5d
```

2) Case 2 :2 digits(two digits)

Example:

Step 1) First LE selects one number ‘q = 97’ such that q ≤ 1 nibble and another number ‘α = 76’ 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 = 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 $Y_A = (((q.\alpha)_* x_B)_* \mathrm{mod}(x_A)) = 12796$ and $Y_B = (((q.\alpha)_* x_A)_* \mathrm{mod}(x_B)) = 4246$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:

$NTBS_A = (((Y_B)(X_A)\ (Y_A)(X_B))_*\mathrm{mod}(Y_B)) = 62393296$ (by node A) and

$NTBS_B = (((Y_A)(X_B)\ (Y_B)(X_A))_*\mathrm{mod}(Y_A)) = 20703496$ (by node B)

Step 6) these common NTBS values transfer to LE.

Step 7) Then LE computes **<u>Final NTBS key</u>** as:

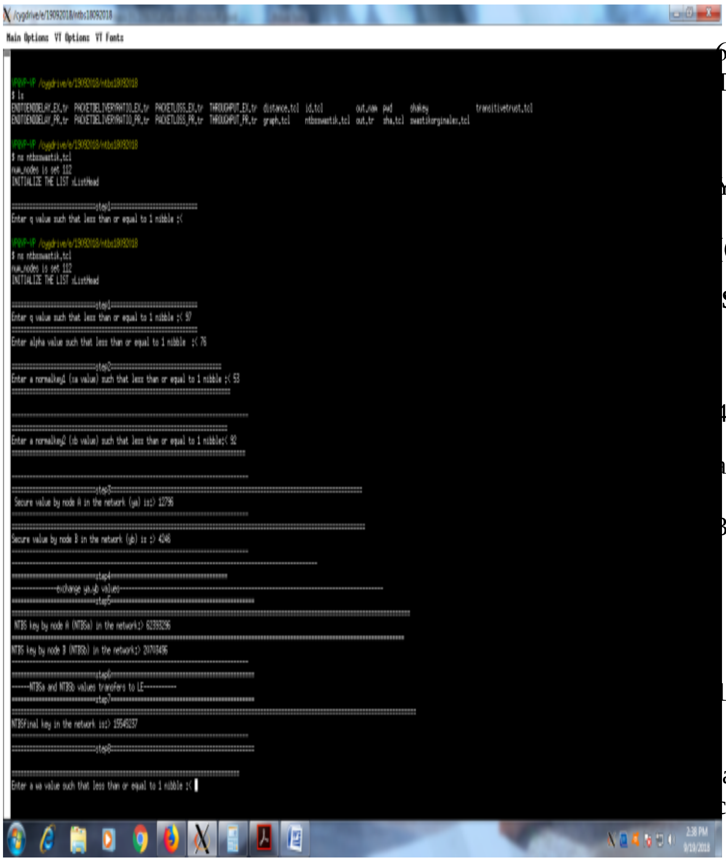
$NTBS_{final} = (NTBS_A{*}\ NTBS_B)$ mod $(NTBS_A{+}\ NTBS_B) = 15545237$

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

TABLE IV. NTBS PROTOCOL KEY GENERATION STEPS WHEN VALUES ARE ≤ 1 NIBBLE

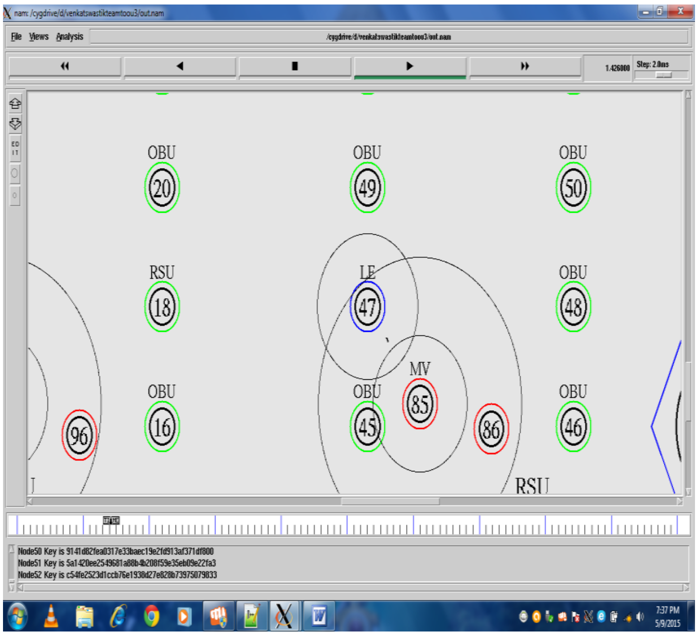
1.Select a number ‘q = 97 ’ such that q ≤ 1 nibble and also Select a number ‘α = 76’ such that α ≤ 1 nibble	
2. node A chooses a key ‘X_A = 53’ such that X_A ≤ 1 nibble node B chooses a key ‘ X_B = 92’ such that X_B ≤ 1nibble and exchange X_A , X_B values	
3. Calculating secure Keys Y_A and Y_B by both nodes and sends to LE	
By node A	By node B
$Y_A = (((q.\alpha)_* x_B)_*\mathrm{mod}(x_A))$ = 12796	$Y_B = (((q.\alpha)_* x_A)_*\mathrm{mod}(x_B))$= 4246
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 ($NTBS_B$)
$NTBS_A$= $(((Y_B)(X_A)$ $(Y_A)(X_B))_*\mathrm{mod}(Y_B))$ = 62393296	$NTBS_B$= $(((Y_A)(X_B)(Y_B)(X_A))_*\mathrm{mod}(Y_A))$ = 20703496
6. these values transfer of common NTBS key to LE	
7. LE calculates $NTBS_{final}$ as : $(NTBS_A{*}Y_B)\ (NTBS_B{*}Y_A)$ mod $(NTBS_A + NTBS_B)$ = 15545237	

a) Key generation steps in NAM: Now lets discuss key generation steps in NAM by using NTBS protocol.



```
X /cygdrive/e/19092018/ntbs18092018
Main Options  VT Options  VT Fonts

VPRVP-VP /cygdrive/e/19092018/ntbs18092018
$ ls
ENDTOENDDELAY_EX.tr  PACKETDELIVERYRATIO_EX.tr  PACKETLOSS_EX.tr  THROUGHPUT_EX.tr  distance.tcl  id.tcl          out.nam  pwd     shakey                 transitivetrust.tcl
ENDTOENDDELAY_PR.tr  PACKETDELIVERYRATIO_PR.tr  PACKETLOSS_PR.tr  THROUGHPUT_PR.tr  graph.tcl     ntbsswastik.tcl  out.tr   sha.tcl  swastikorginalex.tcl

VPRVP-VP /cygdrive/e/19092018/ntbs18092018
$ ns ntbsswastik.tcl
num_nodes is set 112
INITIALIZE THE LIST xListHead

==========================step1==========================
Enter q value such that less than or equal to 1 nibble :(

VPRVP-VP /cygdrive/e/19092018/ntbs18092018
$ ns ntbsswastik.tcl
num_nodes is set 112
INITIALIZE THE LIST xListHead

==========================step1==========================
Enter q value such that less than or equal to 1 nibble :( 97
=========================================================
Enter alpha value such that less than or equal to 1 nibble  :( 76

==========================step2==================================
Enter a normalkey1 (xa value) such that less than or equal to 1 nibble :( 53
====================================================================

-----------------------------------------------------------------------
=================================================================
Enter a normalkey2 (xb value) such that less than or equal to 1 nibble:( 92
======================================================================

-----------------------------------------------------------------------
==========================step3=============================================================================
 Secure value by node A in the network (ya) is:) 12796
-----------------------------------------------------------------------
=============================================================================================================
Secure value by node B in the network (yb) is :) 4246
-----------------------------------------------------------------------
------------------------------------------------------------------------------------------
==========================step4=================================
-------------exchange ya,yb values------------------------------------------------------------------------------
==========================step5====================================
===============================================================================================================================
 NTBS key by node A (NTBSa) in the network:) 62393296
============================================================================================================================
NTBS key by node B (NTBSb) in the network:) 20703496
-----------------------------------------------------------------------
==========================step6====================================
-----NTBSa and NTBSb values transfers to LE----------
==========================step7====================================
=================================================================================================================================
NTBSfinal key in the network is:) 15546237
-----------------------------------------------------------------------
==========================step8====================================

=====================================================================
Enter a wa value such that less than or equal to 1 nibble :(
```

b) Final Communication in NAM: After generating all keys and if we enguage that keys in Nam then final communication would be as follows.



```
Node50 Key is 9141d82fea0317e33baec19e2fd913af371df800
Node51 Key is 5a1420ee2549681a88b4b208f59e35eb09e22fa3
Node52 Key is c54fe2523d1ccb76e1938d27e828b73975079833
```

3) *Case 3 :3 digits(two digits)*

Example:-

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

$Y_A = (((q.\alpha)*x_B)*\text{ mod}(x_A)) = 1005666$ and $Y_B = ((q.\alpha)*x_A)*\text{ mod}(x_B)) = 686574$

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:

$NTBS_A = (((Y_B)(X_A)\ \ (Y_A)(X_B))*\text{mod}(Y_B)) =$ 472403558172 (by node A)

and

$NTBS_B = (((Y_A)(X_B)\ \ (Y_B)(X_A))*\text{mod}(Y_A)) =$ 322512643908 (by node B)

Step 6) these common NTBS values transfer to LE.

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

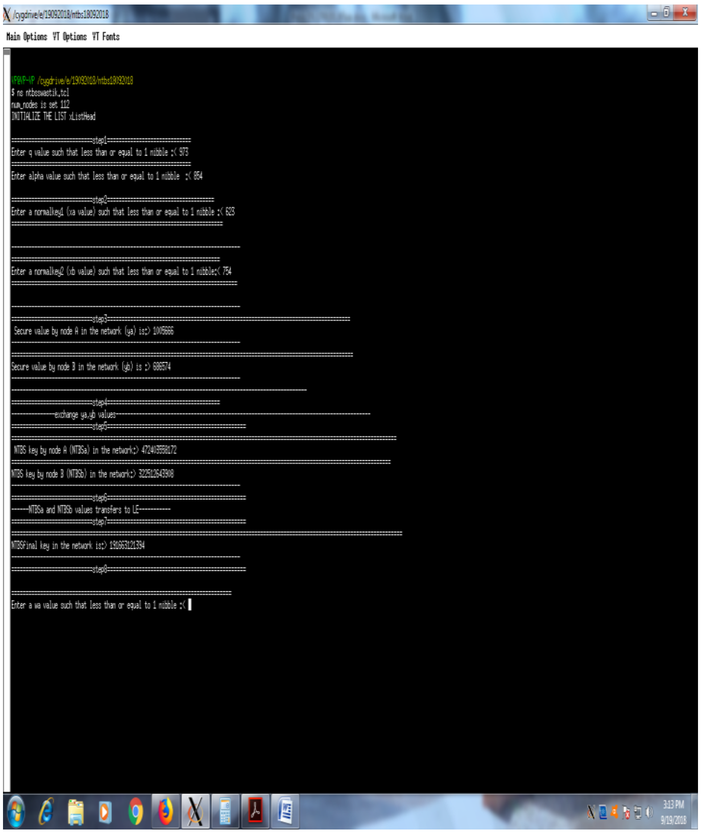
$NTBS_{final} = (NTBS_A* NTBS_B) \text{ mod } (NTBS_A+ NTBS_B) =$ 191663121394

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

TABLE V. NTBS PROTOCOL KEY GENERATION STEPS WHEN VALUES ARE ≤ 1 NIBBLE

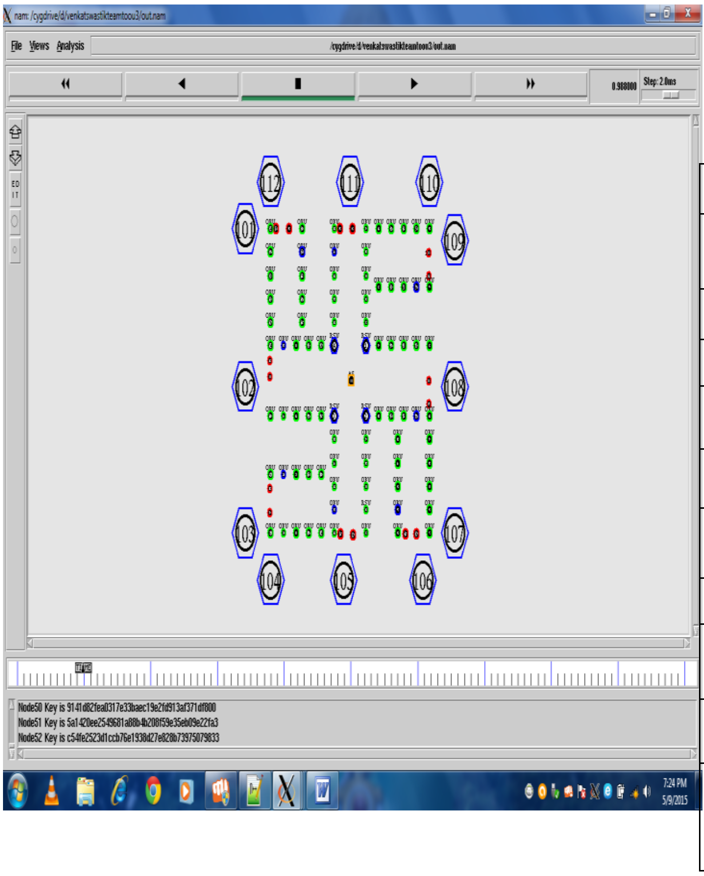
1.Select a number ‘q = 973 ’ such that q ≤ 1 nibble and also Select a number ‘α = 854’ such that α ≤ 1 nibble	
2. node A chooses a key ‘X_A = 623’ such that X_A ≤ 1 nibble node B chooses a key ‘ X_B = 754’ such that X_B ≤ 1nibble and exchange X_A , X_B values	
3. Calculating secure Keys Y_A and Y_B by both nodes and sends to LE	
By node A	By node B
$Y_A=(((q.\alpha)*x_B)*\text{mod}(x_A)) =$ 1005666	$Y_B=(((q.\alpha)*x_A)*\text{mod}(x_B))=$ 686574
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 ($NTBS_B$)
$NTBS_A=$ $(((Y_B)(X_A)\ (Y_A)(X_B))*\text{mod}(Y_B)) =$ 4724035581472	$NTBS_B=$ $(((Y_A)(X_B)(Y_B)(X_A))*\text{mod}(Y_A)) =$ 322512643908
6. these values transfer of common NTBS key to LE	
7. LE calculates $NTBS_{final}$ as : $(NTBS_A*Y_B)\ (NTBS_B*Y_A) \text{ mod } (NTBS_A + NTBS_B) = 191663121394$	

a) Final key generation in NAM: Now lets discuss key generation steps in NAM by using NTBS protocol.



```
\P@\P-\P /cygdrive/e/19092018/ntbs18092018
$ ns ntbsswastik.tcl
num_nodes is set 112
INITIALIZE THE LIST xListHead

========================step1========================
Enter q value such that less than or equal to 1 nibble :( 973
=====================================================
Enter alpha value such that less than or equal to 1 nibble  :( 854

========================step2============================
Enter a normalkey1 (xa value) such that less than or equal to 1 nibble :( 623
===============================================================


-------------------------------------------------------------------
==============================================================
Enter a normalkey2 (xb value) such that less than or equal to 1 nibble:( 754
==================================================================


-------------------------------------------------------------------
========================step3=====================================================================
 Secure value by node A in the network (ya) is:) 1005666
-------------------------------------------------------------------
====================================================================================================
Secure value by node B in the network (yb) is :) 686574
-------------------------------------------------------------------
-------------------------------------------------------------------------------------
========================step4==============================
------------exchange ya,yb values------------------------------------------------------------------
========================step5=======================================
==============================================================================================================
 NTBS key by node A (NTBSa) in the network:) 47240358172
============================================================================================================
NTBS key by node B (NTBSb) in the network:) 322512643908
-------------------------------------------------------------------
========================step6=======================================
-----NTBSa and NTBSb values transfers to LE----------
========================step7=======================================
================================================================================================================
NTBSfinal key in the network is:) 191663121394
-------------------------------------------------------------------
========================step8=======================================

=================================================================
Enter a wa value such that less than or equal to 1 nibble :( ▌
```

b) Final Communication in NAM: After generating all keys and if we engauge that keys in Nam then final communication would be as follows.



nam: /cygdrive/d/venkatswastikteamtoou3/out.nam
File
Views
Analysis
/cygdrive/d/venkatswastikteamtoou3/out.nam
0.988000
Step: 2.0ms
112
111
110
101
109
102
108
103
107
104
105
106
TIME

```
Node50 Key is 9141d82fea0317e33baec19e2fd913af371df800
Node51 Key is 5a1420ee2549681a88b4b208f59e35eb09e22fa3
Node52 Key is c54fe2523d1ccb76e1938d27e828b73975079833
```

4) Case 4 : Nibble(four bits)

Example:-

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

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

Steps 4) then they again exchange secure keys.

Step 5) and both nodes compute NTBS keys as:

$NTBS_A = (((Y_B)(X_A) \quad (Y_A)(X_B))*\text{mod}(Y_B)) = 538287605089850$ (by node A)

and

$NTBS_B = (((Y_A)(X_B) \quad (Y_B)(X_A))*\text{mod}(Y_A)) = 38529750633325$ (by node B)

Step 6) these common NTBS values transfer to LE.

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

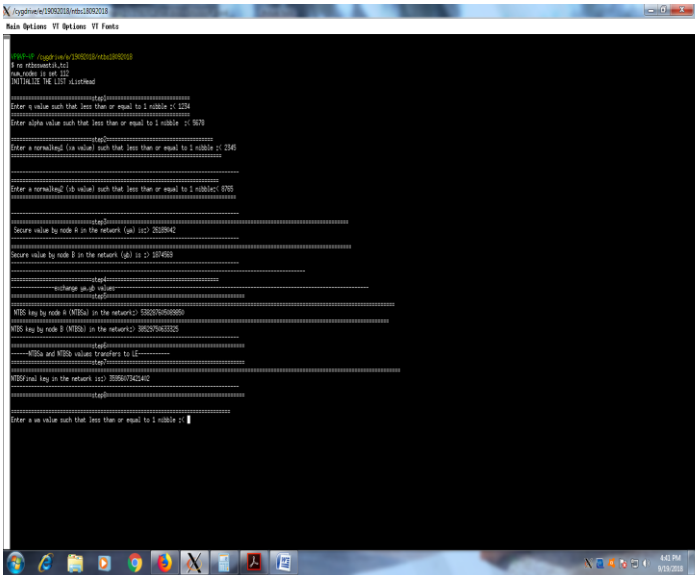
$NTBS_{final} = (NTBS_A* NTBS_B) \text{ mod } (NTBS_A+ NTBS_B) = 35956073421402$

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

TABLE VI. NTBS PROTOCOL KEY GENERATION STEPS WHEN VALUES ARE ≤ 1NIBBLE

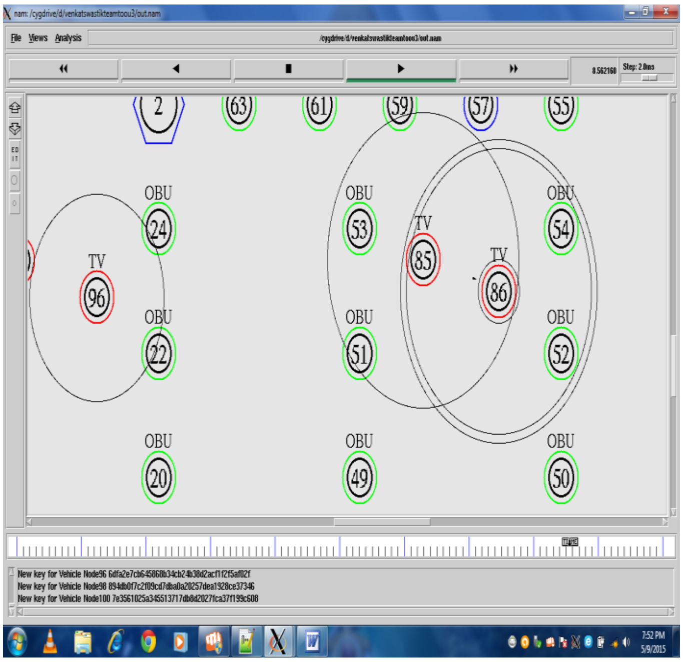
1.Select a number ‘q = 1234 ’ such that q ≤ 1 nibble and also Select a number ‘α = 5678’ such that α ≤ 1 nibble	
2. node A chooses a key ‘X_A = 2345’ such that X_A ≤ 1 nibble node B chooses a key ‘ X_B = 8765’ such that X_B ≤ 1nibble and exchange X_A , X_B values	
3. Calculating secure Keys Y_A and Y_B by both nodes and sends to LE	
By node A	By node B
$Y_A=(((q.\alpha)*x_B)*\text{mod}(x_A))$ = 26189042	$Y_B=(((q.\alpha)*x_A)*\text{mod}(x_B))$= 1874569
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 ($NTBS_B$)
$NTBS_A$= $(((Y_B)(X_A)\ (Y_A)(X_B))*\text{mod}(Y_B))$ = 538287605089850	$NTBS_B$= $(((Y_A)(X_B)(Y_B)(X_A))*\text{mod}(Y_A))$ = 38529750633325
6. these values transfer of common NTBS key to LE	
7. LE calculates $NTBS_{final}$ as : $(NTBS_A*Y_B)\ (NTBS_B*Y_A) \text{ mod } (NTBS_A + NTBS_B)$ = 35956073421402	

a) Final key generation in NAM: Now lets discuss key generation steps in NAM by using NTBS protocol.


/cygdrive/e/19092018/ntbs18092018
Main Options VT Options VT Fonts

```
VP@VP-VP /cygdrive/e/19092018/ntbs18092018
$ ns ntbsswastik,tcl
num_nodes is set 112
INITIALIZE THE LIST xListHead

==========================step1===========================
Enter q value such that less than or equal to 1 nibble :< 1234
==========================================================
Enter alpha value such that less than or equal to 1 nibble  :< 5678

==========================step2=================================
Enter a normalkey1 (xa value) such that less than or equal to 1 nibble :< 2345
==================================================================

------------------------------------------------------------------
==================================================================
Enter a normalkey2 (xb value) such that less than or equal to 1 nibble:< 8765
==================================================================

------------------------------------------------------------------
==========================step3===========================================================
 Secure value by node A in the network (ya) is:> 26189042
------------------------------------------------------------------
==========================================================================================
Secure value by node B in the network (yb) is :> 1874569
------------------------------------------------------------------
------------------------------------------------------------------------------------
==========================step4=================================
--------------exchange ya,yb values-------------------------------------------------------------
==========================step5=====================================
===========================================================================================================
 NTBS key by node A (NTBSa) in the network:> 538287605089850
=========================================================================================================
NTBS key by node B (NTBSb) in the network:> 38529750633325
------------------------------------------------------------------
==========================step6=====================================
------NTBSa and NTBSb values transfers to LE-----------
==========================step7=====================================
============================================================================================================
NTBSfinal key in the network is:> 35956073421402
------------------------------------------------------------------
==========================step8=====================================

=================================================================
Enter a wa value such that less than or equal to 1 nibble :< █
```

b) Final Communication in NAM: After generating all keys and if we engage that keys in Nam then final communication would be as follows.



```
New key for Vehicle Node96 6dfa2e7cb645868b34cb24b38d2acf1f2f5af02f
New key for Vehicle Node98 894db0f7c2f09cd7dba0a20257dea1928ce37346
New key for Vehicle Node100 7e3561025a345513717db8d2027fca37f199c608
```

CONCLUSION AND FUTURE WORK

There is considerable improvement in the data communication between the nodes when secure clustering techniques employed. Without security, the transmission of message information becomes meaningless. These secure clustering techniques are used in security sensitive applications like police and government agencies. Fast communication and security are the major achievements for the VANET system. These play vital roles in obtaining best communication in VANET system environment. In this article we study the proposed scheme called NTBS Protocol to protect valid users in VANET and achieve fast communication requirements in the VANET with security. Among all requirements authentication and privacy are the major issues in VANET system. To give the security to communication is the main idea behind the development of Network Theory Based Secure Clustering protocol which depends on the number theory rules. In this research work we discuss NTBS importance and steps involved in that protocol. To obtain best communication we follow seven steps to authenticate a vehicular node. Finally, we produce a key by utilizing NTBS key generation as well as node authentication.

If we compare the graph results in Xgraph then calculations are substantially better than existing schemes. Moreover, NTBS is depends on the concept of TTRs to improve the communication inside VANET environment by using number theory. In addition, NTBS has a few storage spaces to store the authentication parameters by proposed system because all keys are stored in Authentication Server. NS2 simulations are conducted to verify the proposed scheme, which demonstrates that NTBS clustering protocol yields much better performance.

- In future, new methods not only increasing the communication but also increase the communication range and development of cost-effective VANET system without TTRs concept.
- In future, new protocol mechanism standards will be explored using number theory to avoid disconnection in network because of fast topology.
- In future, a mechanism developed to avoid frequent disconnection in network because of fast topology based on number theory.

REFERENCES

[1] National Highway Traffic safety Administration, [Online], Available: http: //www.nhtsa.gov

[2] Dargay, and H. Huntington, ”Vehicle ownership and income growth, worldwide: 1960-2030”, in The Energy Journal, vol. **28**, No. **4**, **2007**.

[3] Sabih ur Rahman, M. Arif Khan, Tanveer A. Zia, and Lihong Zheng,*“ Vehicular Ad hoc Networks (VANETs)- An Overview and Challenges”,* Journal of Wireless Networking and Communications, vol. **3**, no. **3**, pp. **29-38**, **2013**.

[4] Venkatamangarao Nampally, Dr. M. Raghavender Sharma, “*Invention and Implementation of NTBS Clustering Protocol for VANET”,* International Journal of Computer Sciences and Engineering (IJCSE), Vol.**6**, Issue.**5**, pp.**1100-1110**, **2018**.

[5] Venkatamangarao Nampally et al, Dr. M. Raghavender Sharma, *“A Survey on Security Attacks for VANET”*, International Journal of Computer Science and Mobile Applications (IJCSMA), Vol.**5**, Issue.**10**, pp.**58-70**, **2017**.

[6] 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**.

[7] Walter Franz, Hannes Hartenstein, and Martin Mauve, *“Inter-Vehicle-Communications based on Ad Hoc Networking Principles”,* The FleetNet Project, **2005**.

[8] Sabih ur Rahman, M. Arif Khan, Tanveer A. Zia, and Lihong Zheng,*“ Vehicular Ad hoc Networks (VANETs)- An Overview and Challenges”,* Journal of Wireless Networking and Communications, vol. **3**, no. **3**, pp. **29-38**, **2013**.

[9] Venkatamangarao Nampally, Dr. M. Raghavender Sharma, *“Information sharing standards in communication for VANET”,* International Journal of Scientific Research in Computer Science Applications and Management Studies (IJSRCSAMS), Vol. **7**, Issue. **4**, **2018,** ISSN: **2319-1953**, GIF: **0.6**.

[10] Venkatamangarao Nampally, Dr. M. Raghavender Sharma , *“Increasing Information Shareability by Using NTBS Clustering*

Approach for VANET”, IPASJ International Journal of Computer Science (IIJCS), Vol.**5,** Issue.**10**, pp.**1-17**, **2017**.

[11] M. Gerlach, and VaneSe , *“ An Approach to VANET Security”*, in the proceedings of V2VCOM, **2005**.

[12] 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**.

[13] 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**.

[14] K. Madhurima, and P. Kalyani, *“Accelarate TESLA Protocol for VANET”,* International Journal of Research and Computational Technology, vol. **6**, issue. **2**, **2014**.

[15] Amarpreet singh, and Manverpreet Kaur, *“ A Novel Clustering Scheme in Vehicular Ad hoc Network”*, International Journal of Applied Information Systems (IJAIS), Volume. **10**, no. **3**, **2015**.

[16] Menezes, S. Vnstone, and D. Hankerson,*“Guide to elliptic curve cryptography”,* Spinger Professional Computing (Springer, New York 2004)

[17] 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**.

[18] 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**.

[19] 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**.

[20] 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**.

[21] S. Sivagurunathan, P. Subathra, V. Mohan, N. Ramaraj, *“Authentic Vehicular Environment Using a Cluster based Key Management”*, Eur. J. Sci. Res.,vol. **36**, pp. **299–307**, **2009**.

[22] 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**.

[23] 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**.

[24] O. Kayis, and T. Acarman, *“ Clustering formation for inter vehicle communication”*, In Intelligent Transportation Systems Conference, ITSC 2007, IEEE, pp. **636-641**, **2007**.

[25] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, *"An Identity based Security System for User Privacy in Vehicular Ad Hoc Networks"*, Parallel and Distributed Systems, IEEE Transactions, vol. **21**, no.**9**, pp.**1227-1239**, **2010**.

[26] 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**.

[27] Kamlesh Namdev, and Prashant Singh, *“ Clustering in Vehicular Ad Hoc Network for efficient Communication”,* International Journal of Computer applications, vol. **115**, no. **11**, pp. **15-18**, **2015**.

[28] 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**.

[29] T. D. C. Little, and A. Agarwal, *“ An Information Propagation Scheme for VANET”,* in the proceedings of the IEEE Intelligent Transportation systems, pp. **155-160**, **2005**.