ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture

Prabhakar Manish, Dr. Vaishali Khairnar

M.E. Student, Dept. of I.T., Terna Engineering College, Nerul, Mumbai University, India

HOD, Dept. of I.T, Terna Engineering College, Nerul, Mumbai University, India

ABSTRACT: In VANET networks, vehicles communicate with each other and possibly with a roadside unit to provide a long list of applications such as, transit safety, driver assistance and internet access. In VANET networks, knowledge of the real-time position of nodes is an assumption made by most protocols, algorithms, and applications. Recently, VANETs have emerged to turn the attention of researchers in the field of wireless and mobile communications; they differ from MANET by their architecture, challenges, characteristics and applications. VANETs are distinguished from other kinds of ad-hocnetworks by their hybrid network architectures, node movement characteristics, and new application scenarios. VANETs pose many unique networking research challenges, and the design of an efficient routing protocol for VANETs is thus, very crucial. This paper presents, system to understand and distinguish the main features, surrounding VANET in a single unit, that help us to understand how the use of ad-hoc network improves the signal strength along with providing the security to the VANET with cloud environment.Here we present VANET simulation with the cloud connectivity and their analysis to improve the signal level and QoS parameter, for the VANET network.

KEYWORDS: VuC; RSU; Cloud; VANET; EMAP Protocol; Ad Hoc Network; Network Security.

I. INTRODUCTION

The wide deployment and evolution of wireless communication systems have changed human lives by offering easiness and flexibility in using internet services and various applications. In ad-hoc network, mobile nodes self-organize themselves to create a network without the support of any infrastructure like base-stations. Cloud computing is supposed to be the next big thing because of its scalability, PaaS, IaaS, SaaS and other important characteristics [1]. A Vehicular Ad-hoc Network (VANET) is used to provide convenient wireless network services. Researchers have abstracted the idea of VANETs, in which vehicles, equipped with wireless communication devices, positioning systems, and digital maps, act as intelligent machines that communicate for safety and comfort purposes [2]. VANETs allow vehicles to connect to Roadside Units (RSUs), which are fixed infrastructure that are equipped with powerful computing devices and installed at different locations in a city[2]. In addition, when VANET is installed in vehicles, they will act as Vehicle Using Cloud (VuC) that increases the signal strength andquality of service (QoS) parameter for the existing VANET.

When VuC provide the infrastructure locally for the nearest vehicle in their range, the vehicle should be authenticate by the trusted authority and for that this paper uses the HMAC authentication protocol for the Vehicular ad hoc network to fulfil the security criteria in the effective manner. The concept of this paper will describes the complete simulation environment to create ad hoc network and, provide the road side unit (RSU) communication, Vehicle to Infrastructure communication (VIC), Vehicle to Vehicle communication with the help of VuC increases the signal strength of the ad hoc network, decrease the message loss ratio and improve the QoS parameter.

VANET is a vehicular communication network which has transformed the transportation systems. The vehicles and RSU's in VANET act as communicating nodes exchanging the information such as traffic, safety etc. via the Wireless Local Area Network (WLAN). The vehicles and RSU'scommunicate with each other in two basic communication modes such as Vehicle-to-vehicle (V2V) and vehicle-to infrastructure (V2I). VANET possesses various characteristics such as mobility, dynamic in nature, real time processing, self-organizing of the nodes etc. The main goal of VANET is to provide safe, comfortable drive and offer safety measures in traffic. Vehicle-to-Vehicle (V2V) and vehicle-to-infrastructure (V2I) allows the VuC's to communicate with each other and with RSU's using wireless technology. V2V

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

and V2I have various attacks such as injecting false information, modifying and replaying the disseminated messages etc. Thus, securing of the VANET is necessary before deploying it in real time [3].

II. RELATED WORK

Authors in [1] say, while on the road if there is no base stations nearby, there is not a problem because due to the ad-hoc network structure all the nodes create a network by hopping the signal eventually to the nearest base stations. Moreover, through VANET, each vehicle can communicate with the other vehicle through V2V network. So, with the ad-hoc network created within the vehicles, traffic can be controlled. Whenever a car will come into a close proximity within a certain region which can make congestion in the road, by V2V the car will send message to the other car and create enough room in the road so that when the green signal turns on every car can move comfortably without making a huge traffic jam due to congestion. The front vehicle constantly sends a communication message for keeping a distance to the rear vehicle and issues a warning message in case of violation [2]. This also helps traffic administration to control and mitigate accidents and identify the mistakes for legal actions.

In [3,6], the architecture of proposed VuC system consist of Trusted Authority (TA), Road Side Unit (RSUs) and On-Board Units (OBUs). Trusted Authority (TA) is responsible for providing the certificate and distributing secret keys to all OBUs in the network. RSUs are fixed units distributed all over the network which can communicatesecurely with the TA. OBUs can communicate with other OBUs through Vehicle-to-Vehicle communication or with RSUs through Vehicle-to-Infrastructure communications[4]. Vehicle to vehicle communication is possible only when the distance between the vehicles is within minimum transmission range. Trusted Authority (TA) assigns each vehicle the hash key for their communication and vehicle generate the HMAC using the hash key obtained by the TA. The vehicle then requests the access point (RSUs) for the desire file[5]. The access point in turn verifies the hashed key of the vehicle with the TA using HMAC[6]. If the verification is successful then vehicle is allowed to access the file in the cloud else else vehicle is denied the access [9].

III. PROPOSED SYSTEM

A. *Design Considerations:*

In this model, we propose to use the vehicles on which wireless device are mounted and these vehicle is authorized to use Cloud Services through base station, in the city as the backbone of the network. These vehicles act as the Vehicle Using Cloud (VuC), The only fixed part of the network infrastructure are Road Side Unite (RSU) that are the small number of base station nodes and due to the multi hop routing capacity of the ad hoc network mobile backbone nodes, placement of the fixed base station nodes is significantly simplified [1]. The network thus forms a hierarchical, multitier structure. Network mobile nodes route packets between personal mobile nodes within the ad hoc network, and between personal mobile nodes and the internet, through a small set of fixed base stations [1].

So while vehicle moving on road if there is no RSU in nearby, there is actually not a problem because due to the ad hoc network structure all the VuC nodes create a network by hopping the signals eventually to the nearest RSU. Moreover, through VANET, each vehicle can communicate with the other vehicle through V2V network and Vehicles are also able to use the internet & calling services by proper authentication using EMAP authentication protocol.

System improves the Quality of Service (QoS) by improving the network coverage, Actually the VuC has the higher capacity device with higher power radiation so that communicates with the RSU while distance is increase and it will provide the coverage to the vehicle that belongs to their nearby area.

This system will able to increase the RF signal coverage up to 30 percent of the fixed RSU network infrastructure, it is also able to calculate the percentage of loss due to the coverage loss.

The architecture of the “Cloud computing in VANET to create Ad Hoc network Architecture” as depicted in Figure. 2 consist of Road Side Unit (RSU), On-Board Unit (OBU), Vehicle using Cloud (VuC), and Trusted Authority (TA)

- Initial RSUs are fixed Node and VuC are moving vehicle.
- All vehicles generate its Time stamp, Private Key and public key.
- Keeping track of previously used connectivity.
- Considered all possible paths at beginning.
- The no signal is available find alternative solution.
- Calculate message loss ratio.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

B. *System Flow Chart:*

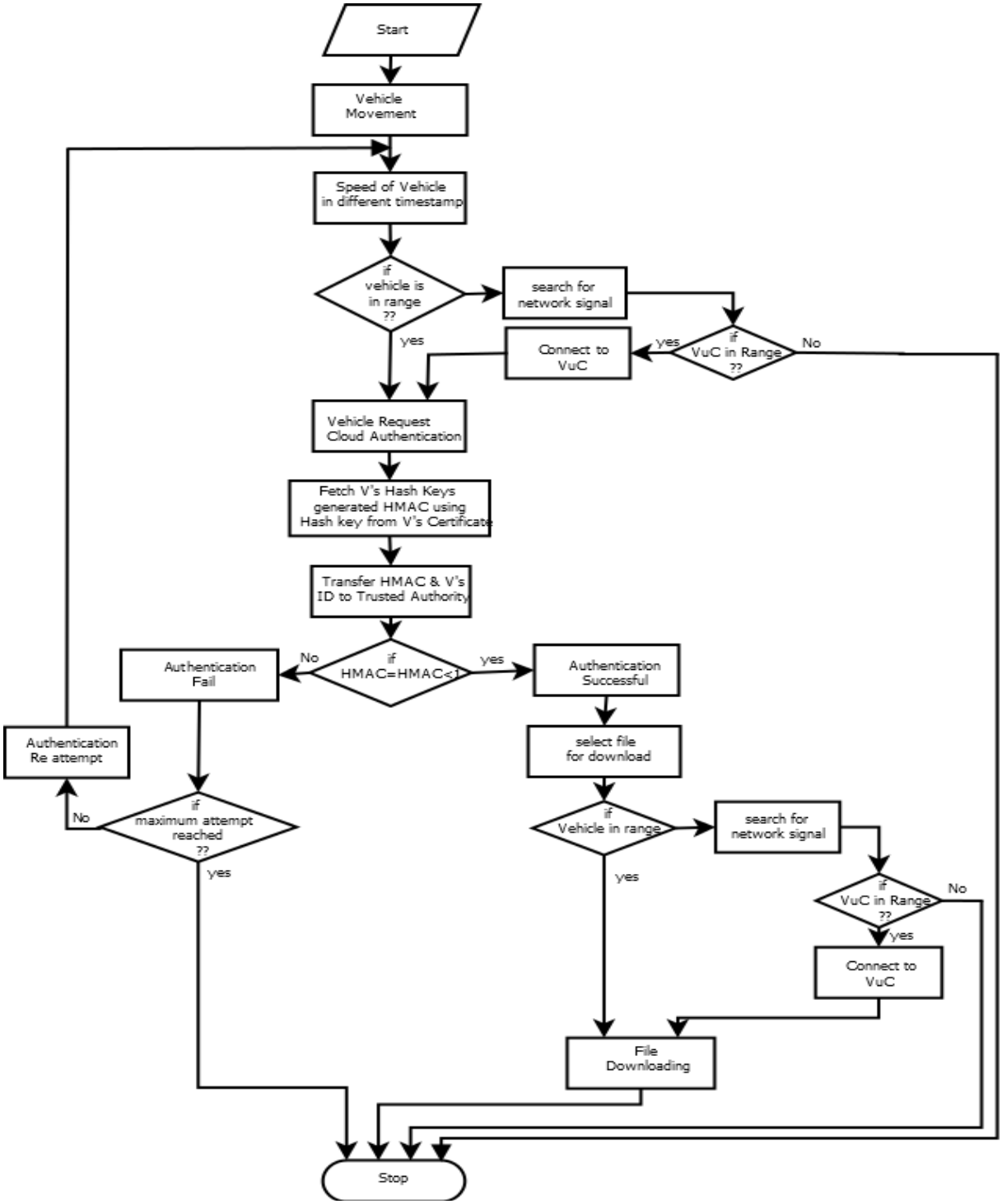

Figure.1 System Flow charts.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

C. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to maximize the network coverage and combine Cloud with VANET by improving the signal strength with secure EMAP authentication protocol. The proposed algorithm is consists of three main module.

Step 1: **Calculating Free-space RF Propagation:**

The free-space loss on LOS calculated by using eq.(1)[16].

$$Lp = 32.4 + 20 \log_{10} f + 10n \log_{10} deq. \quad (1)$$

The frequency of transmission f is specified in MHz and the distance d is specified in kilometers. Tthe higher the transmission frequency, the higher the propagation loss is for the same distanceand parameter n is known as the path loss exponent.

Step 2: **EMAP Authentication And Message Signing process:**

Step1: Before any VuC broadcast Message M, it calculate its Rv_{check}

$Rv_{check}=HMAC(K_p, VIDu||T_{stmp})$

Where HMAC is Hash message authentication code, Kp is the Private key, VIDu is Vehicle ID, Tstmt is timestamp.

Step 3: **Any VuC receive the message**

M||Tstmp||Cert(VID,Kp,Sign(VID||PKu))||Rvcheck and Kp

Can do the message verification as follows:

1: Check timestamp validity
2: **if** invalid **then**
3: Authentication Fail
4: **else**
5: **verify the TA signature on CERT**$_{VuC}$
6: **if** invalid **then**
7: Authentication Fail
8: **else**
9: verify the signature **sign**$_u(M||T_{stmp})$using VuC public keyPKu
10: checkRv_{check}= $HMAC(K_p, VID||T_{stmp})$
11: **if** invalid then
12:Authentication Fail
13: **else**
14:Stop process
15: **end if**
16: **end if**
17: **end if**

IV. IMPLEMENTATION

The proposed architecture is implemented using ASP .Net Language, MySQL Database and public cloud called Microsoft Azure Cloud platform. The user interface is created in C#.

Message Broadcast and receive Module: This system module implemented to synchronize the RSUs or VuC to the vehicle together to keep track of message broadcast and message received by individual vehicles and this can be done my calling messageBroadcast(). IF RSU sending broadcast message and corresponding vehicle unable to receive that message then nearest VuC will approach vehicle to take handover and continue transmission.

RF range Calculation : This system architecture mainly deal with calculating the signal strength on every time quantum t and report to RSU and send information to server for static analysis and this will done by calling calculateValue() andcalculateWidth(). It simply calculates RF behavioral parameter and calculate the signal strength

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

and invoke handover. Handover done when signal strength decreases below threshold level and other RSU or VuC is available in range.

*Authentication to cloud:*This module invoke server to authenticate the vehicle by simply calling the authenticateClient() and once the Vehicle authenticated they are globally authorized to access and download the file and this has been done bycallingauthenticateClient(). This module mainly perform the cloud authentication process to use the cloud services on VANET.

File Download: This module contain web services to interact vehicle to cloud for file download process by calling downloadFile(). This module provides the facility to pause downloading process or kill downloading process. Downloading Pause happen when no network coverage in moving vehicle and whenever comes in network coverage its started download process and when the time expired then its stop the downloading process.

Graph Generation: System module uses for statically analysis that comprises all the activity including RF Behavior, signal strength, message broadcasts and message file download module process by calling graphAnalysis() function.
In this section we provide the following graph.

1. Signal strength graph.
2. Throughput graph.
3. Individual Vehicle graph with RSUs Vs RSUs with VuC.
4. Message loss ratio graph.

V. SIMULATION RESULTS ANALYSIS

The simulation studies involve the deterministic small network topology with 4 vehicles, 2 RSUs and 2 Vehicles as shown in Fig.1. The proposed energy efficient algorithm is implemented with .Net. We transmitted same size of data packets through RSUs to destination all 4 vehicle node. System algorithm is compared between two metrics signalstrength with RSUsand signal strength with RSU along with VuC, No of message broadcasted and no of message received. We considered the simulation time as a network lifetime and network lifetime is a time when no route is available to move the vehicles. Simulation time is calculated through the Stopwatch class of C#. Our results shows that the RSUs along with VuCs performs better signal strength than the signal strength with RSUs, total no of broadcast message received with RSUs along with VuCs and total number message received through the RSUs only.

The network showed in Fig.3.is able to provide the system throughput by callingthroughtputGraph(). It clearly shows in Fig. 2 that the metric total network coverage maximum by VuC in association with RSUs than network coverage provided by traditional RSU. As the network is VANET means nodes are vehicle and they change their locations with respect to time. After nodes have changed their location the new topology is shown in Fig.3.and message success ratio of each node is shown in Fig.4. Our results show that throughput and message success ratio performs better than the traditional VANET network with RSU that improves QoS parameter.Fig.5. shows the cloud authentication model for the VANET, All the vehicle registered with the server by giving its identity i.e. VID, Timestamp, Private key Public key, Revcheck() that stores the all information to cloud for authentication. From Fig.5 clearly shows the authentication process.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

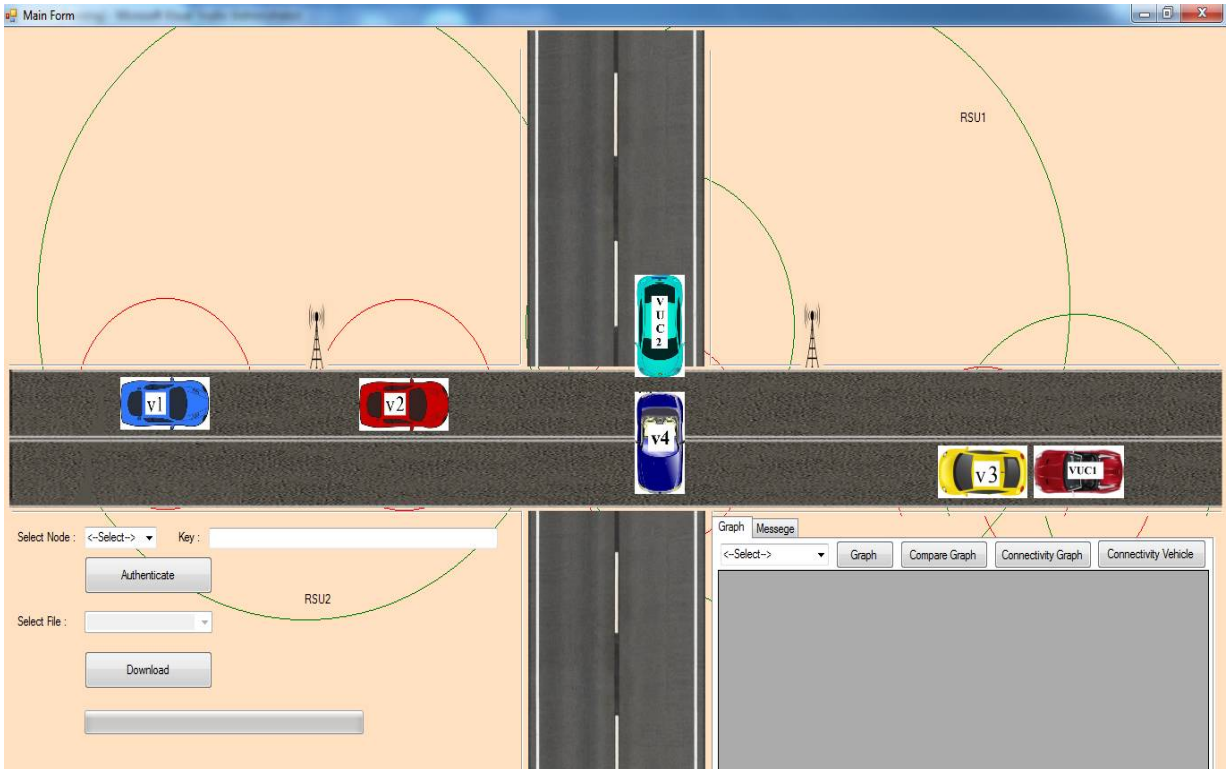

Fig.2. RF Simulation signal environment with 2 RSUs, 2 VuCs and 4 Vehicles node

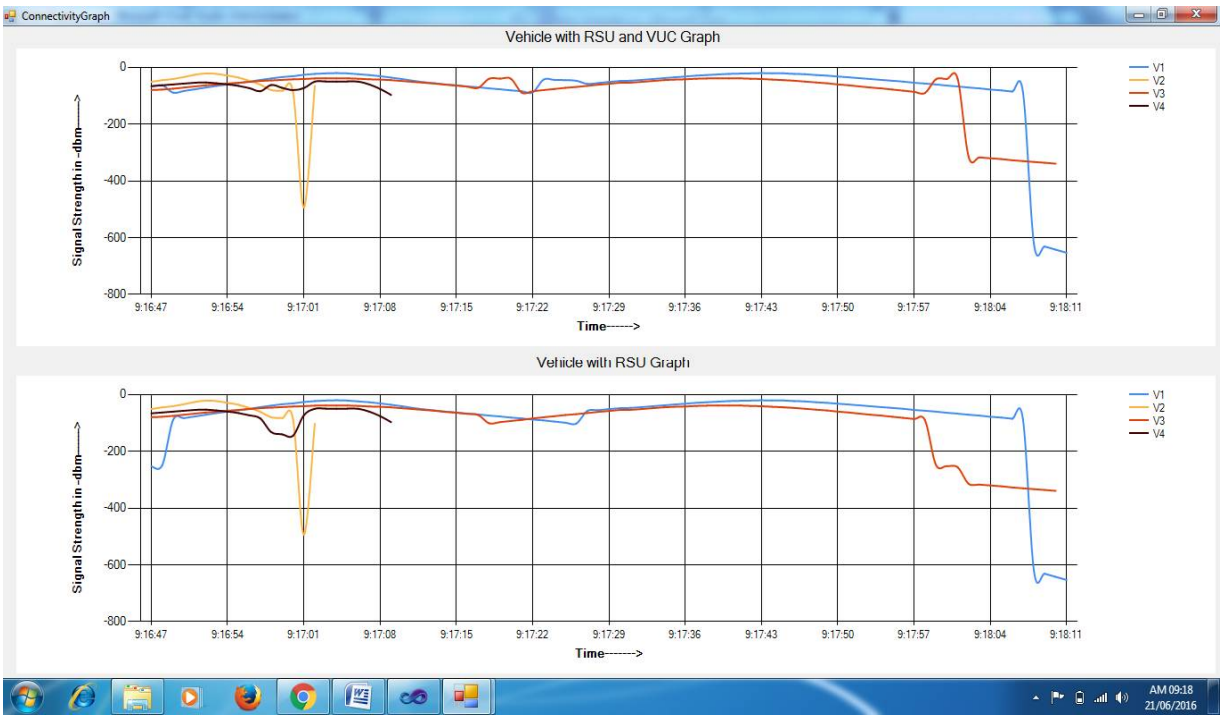

Fig. 3. System Throughput graph.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

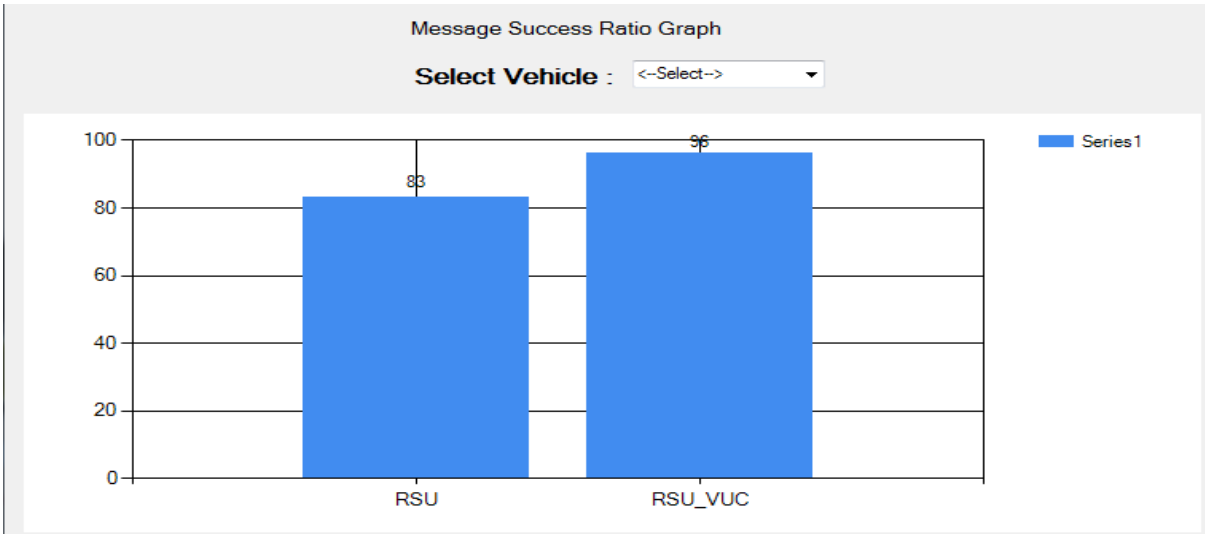

Fig. 4. Message Success Ratio

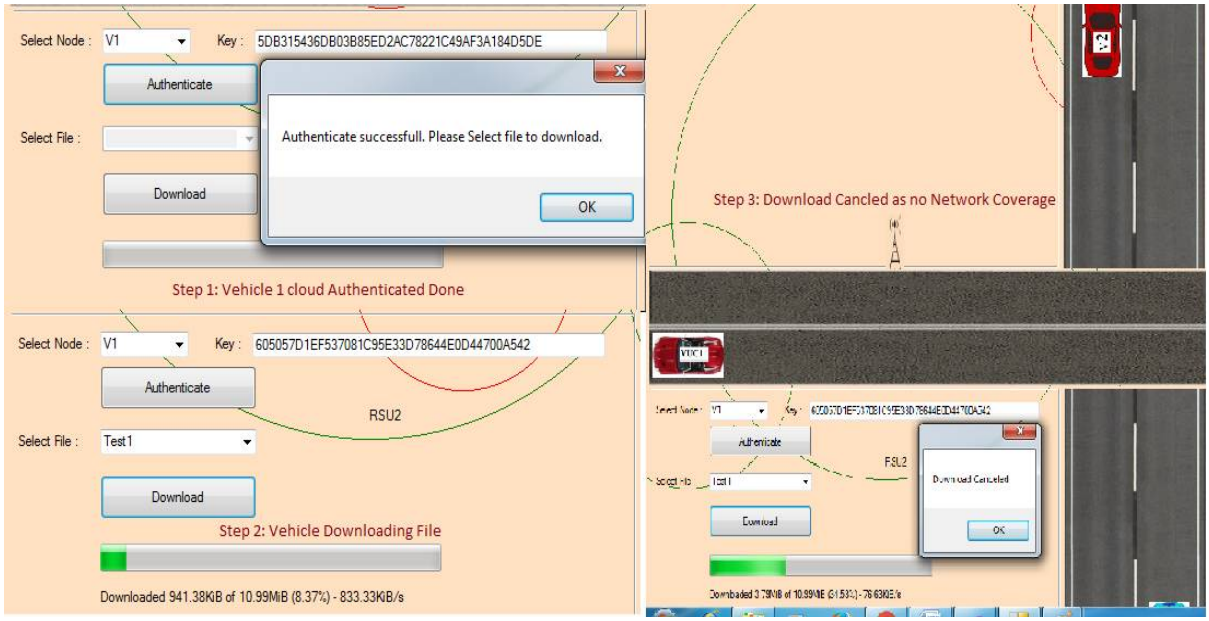

Fig. 5. Vehicle Authentication process by EMAP Protocol.

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the algorithm performs better throughput with the RSUs along with VuC than throughput with RSUs. The algorithm provides better message transmission ratio for data transmission and maximizes the lifetime of entire network. This system combined Vehicular Ad-hock Network (VANET) with cloud with EMAP authentication protocol.As the performance of the algorithm is analyzed between two metrics in future with some modifications in design considerations the performance of the algorithm can be compared with other Cloud message Authentication efficient algorithm. We have used very small network of 4 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

REFERENCES

1. Md Ali Al Mamun, KhairulAnam, MdFakhrulAlamOnik and A M Esfar- E- Alam, "Deployment of Cloud Computing into VANET to Create Ad Hoc Cloud Network Architecture", Proceedings of the World Congress on Engineering and Computer Science, ISBN: 978-988-19251-6-9, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online), Vol. I, 2012.
2. AshwiniAbhale, SumitKhandelwal and Uma Nagaraj, "Shifting VANET to Cloud - Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 11, 2013.
3. C Shravanthi and H S Guruprasad, " VANET using Cloud [VuC]", IPASJ International Journal of Information Technology, Vol. 2, Issue 6, 2014.
4. JyotiMetan1, K N Narasimha Murthy and Jithrendra H N, "Moving VANET to Vehicular Cloud", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 2, Special Issue 2, 2014.
5. Sayeda Ayesha Parveen, "Security in VANET using EMAP", International Journal of Computer & Mathematical Sciences, Vol. 3, Issue 9, 2014.
6. AspariNagaraju, Om Prakash and K. Prasanth Kumar, "EMAP: EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS", International Journal of Engineering & Science Research, Vol. 4, Issue 10, pp. 569-573, 2014.
7. ShraddhaGajare and Nilima Nikam, "Expedite Message Authentication Protocol", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 12, 2014.
8. Santhosh Kumar B.J and Amrita VishwaVidyapeetham, "Fast and Secure Message Authentication Protocol Using Hmac for Vanets", International Journal of Advanced Research in Computer Science and Software Engineering, Issue 4, pp. 731-736, 2015.
9. 9 C.SelvaLakshmi, N.SenthilMadasamy and T.Pandiarajan, "Secured Multi Message Authentication Protocol for Vehicular Communication", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 12, 2013.
10. Euisin Lee, Eun-Kyu Lee, Soon Y. Oh, and Mario Gerla, "Vehicular Cloud Networking: Architecture and Design Principles".
11. Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", pp. 393-398, 2010.
12. Yipin Sun,Rongxing Lu,Xiaodong Lin, Xuemin (Sherman) Shen, and Jinshu Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications", IEEE Transactions On Vehicular Technology, 2010.
13. Qing Xu, Tony Mak and Raja Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC", ACM 1-58113-922-5/04/0010, 2004.
14. Albert Wasef, Yixin Jiang, and Xuemin Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks", IEEE Transactions On Vehicular Technology, Vol. 59, No. 2, 2010.
15. Lot_ ben Othmane, Harold We_ers, MohdMurtadha Mohamad, and Marko Wolf, "A Survey of Security and Privacy in Connected Vehicles".
16. Purnima K. Sharma and R. K. Singh, "Cell Coverage Area and Link Budget Calculations in GSM System", International Journal of Modern Engineering Research, Vol. 2, Issue.2, pp-170-176, 2012.

BIOGRAPHY

Prabhakar Manish, Master of Engineering (ME) Student in the Information Technology Department, Terna Engineering College, Nerul Navi Mumbai, University of Mumbai, India

Dr. Vaishali Khairnar, Head of Department, Information Technology, Terna Engineering college, Nerul, Navi Mumbai, India