# To Enhance Security in VANET using Adaptive Algorithm

**Namarpreet kaur, Aman Arora**

***Abstract*— Vehicular Ad hoc Networks (VANETs) are the promising approach to provide safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security in VANET got less attention. In this article, we have discussed about the VANET and its technical and security challenges. We have also discussed some major attacks and solutions that can be implemented against these attacks. We have compared the solution using Algorithm Passing parameters.**

***Index Terms*— VANETs, Vanet security, Adaptive Algorithm, Denial of Service.**

## I. INTRODUCTION

As the use of Wireless technology goes on increasing People can use wireless technology everywhere means at café, hotels, etc. Thus due to this many cars manufacturers and telecommunication industries have to teamed with each other so that the car is equipped with wireless technology . Vanet provides many IT services to the Vehicles and it also deals mainly with Security. Cars that are equipped with Wireless technology and Road Side Unit form a network called Vanet [1]. To improve the Performance of Vanet many standards and Protocols has been used . To improve the Performance SPAM Signcryption Message Authentication protocol (SMAP) has been used. It provides message confidentiality integrity etc.It also replces CRL by HMAC function in order to avoid authentication delay due to CRL checking [2].

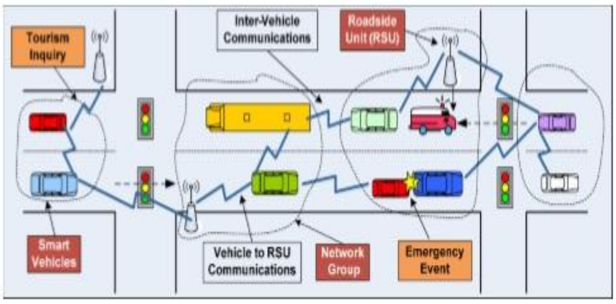


Fig 1 : Basic Structure Of Vanet [3]

### Mobility Models Features

A mobility models define the set of rules that represents the movement of nodes used by network simulator in order to create topologies and some work has been done between them[4] **.**

1. **Mobile Sim :** Mobile Sim is a Mobility Model that sends GDF as input and get Qualnet and ns-2 as output. Its Platform is Java and it is user defined.
2. **STRAW :** It is another mobility model the input provided to it is TIGER and get Swan as Output . Its platform is strawn and it defines geographically[4]**.**

### Recent Project to Encourage vanet

Many projects has been recently introduced most recent Project is Project on Wheels .This Project is found by Daimel Chrysler and its aim is to Provide Security among nodes and solve all the technical issues of communication Channels [5].

In Vanet the communication between the nodes has done directly which affects its Security . In order to provide proper Security the vehicle has full knowledge about its neighbouring Vehicles Thus in order to get Proper knowledge about neighbouring vehicles novel protocls has been used which is used to improve applications that are affected by moving vehicles [6]

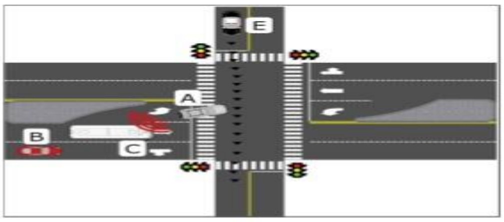


Fig 2 : Vehicle awareness that improves the applications that are affected by moving vehicles[6]

### STATE OF THE ART REGARDING VANET AND VANET-BASED CLOUDS

The most research work on Vanet has been Carried out the research work in vanet is related to its development , Privacy,Security etcbut the main Concern of Vanet is its Security because the Vanet Communication has been done in Wireless Communication Thus it is very important to secure the data that is shared among different nodes in Wireless Communication . Vanet not only provides Safety and Non-Safety applications but it also Provide Value added Services like online Toll Payement ,Movie on demand etc but as the advancement in technology takes place resources become unlimited and this problem has been overcome by Cloud Computing .Thus in future Whwn Cloud Computing and Vanet technologies are Combined it will get more benefits[7]

### Channels in DSRC

These are the Channels of Dedicated Short range Communication which are helpful in Providing safety to communication Channel in which the node communicate.In

**Namarpreet kaur,**Student, M.Tech (CSE), PTU
**Aman Arora,** Head of Department, PTU

this Channels Service ,Control,Long range Channels,Accident avoidance Channels are included [8].

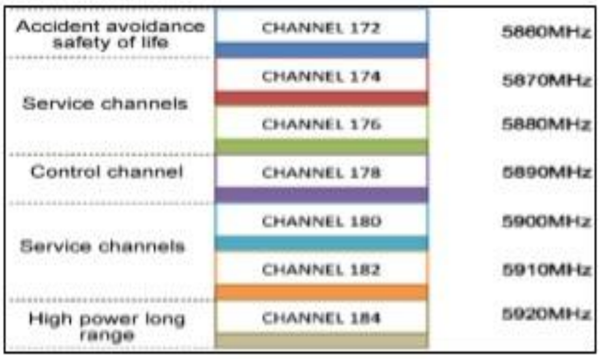


**Fig 3 : Seven Channels in DSRC[8]**

**Performance Analysis of One of the Major Attack in Vanet Called Blackhole Attack[9]**

Black hole Attack is one of the Major Attack in Vanet in case of Computer networks thus in this we have to deal with various performance measure in order to evaluate Black hole Attack which is the major issue and all other Attacks .The performance of different Attacks can be evaluated depend on network throughput and network load. In this we also deal with the different solutions in order to avoid this attack in vanet [9].

## II. Related work

Tamil Selvan [10] says that Vanet is the emerging area of MANET. In Vanet Communication Vehicles have to communicate with Other Vehicles means in this Vehicle act as a nodes. As Vanet Communication takes place under Wireless Channel Thus it is very important to Provide Security to Vanet nodes . Vanet Provides us many security as Well as Value added applications thus it plays a important role in our lifes. Vanet also profide Comforts to drivers of cars Who take part in Communication and it also provide many other services like online toll Payement,Avoid Accidents etc. As Vanet Provides us many Services it also Provide many Challenges Such as security , Integrity etc. But Provide Security to Vanet is one of the Important Challenge . We provide Security by giving user authentication certificates etc . In this paper Selvan also discuss various attacks in Vanet . Thus in order to avoid Security Problems Selvan Proposed light weight Holistic Protocol for Secure data transmission in Vanet [10].

R Saranya [2] provides vanet Security by using Public key infrastructure and Certification Revocation list Which contains the list of certificates and also contain Certification holder names. In PKI system First of all signatures of sender and his or her Certificate is Checked from Certification revocation list So that it assures that the message is received by authorize receiver and message is Send by authorize sender.In this Paper SMAP Protocol is used Which combines digital signature and encryption technique is combined to provide Security. It also Provide message verification Scheme with the help of which message loss ratio decreases .Thus Saranya Proved that SMAP is Secure and efficient algo in providing Security

Vinh Hoa La [3] found Vanet is one of the advance and important topic today. As it provides many benefits such as Provide Drivers Comfort etc.But there are some challenging Attacks in Vanet .In this Papers Various Attacks and Solutions are discuss

## III. Results Analysis

**Proposed Schema :** The authentication protocol based on Hybrid Signature (HS) scheme is a combination of BP and GS Each node V is equipped with a group signing key gskV and the group public key GPKCA (total of vehicles registered with the CA). Rather than generating group signatures to protect messages, a node generates its own set of pseudonyms (according to the BP public key cryptosystem). For HS, the CA does not provide a certificate on Ki V ; V uses gskV to generate a group signature CA,V (Ki V ) on each pseudonym Ki V instead. V attaches ΣCA,V (Ki V ) to each message, and signs with the corresponding k i V to generate the following message format . V −→ ∗ : m, σk i V (m), Ki V , ΣCA,V (Ki V ) When a node receives a message, the group signature CA,V (Ki V ) is verified, using GPKCA. If successful, the receiver infers that a legitimate group member generated pseudonym Ki V . As per the properties of group signatures, the receiver/verifier of the certificate cannot identify V and cannot link this certificate and pseudonym to any prior pseudonym used by V . Once the legitimacy of the pseudonym is established, the validation of σk i V (m) is done. To identify the message signer, an Open operation on the CA,V (Ki V ) group signature is done; message m is bound to Ki V via σk i V (m), and Ki V is bound to V via CA,V (Ki V ) Optimizations are done to reduce protocol overheads. In the case of optimization in HS at the sender side, the CA ,V (Ki V ) is computed only once per Ki V , because CA, V (Ki V ) remains unchanged throughout the pseudonym period t. The sender appends CA, V (Ki V ) to all messages. At the verifier's side the CA, V (Ki V ) is validated upon the first reception and stored. For all subsequent receptions, if CA, V (Ki V ) has already been verified, the receiver skips its validation. Optimized HS will be considered for performance analysis. Primarily, the two scenarios, highway and congestion, will be considered for performance analysis. The different parameter values of both scenarios are given in Table 6.1, derived Value of message sizs are chosen to correspond to a maximum message size of 1100 bytes, as per the message range**.** chosen in The minimum DSRC channel capacity of 6 Mbps for safety messages will be considered. The following parameters are defined for further use in performance analysis

m =total message size (bytes)

s = safety message size (bytes)

o = cryptographic overheads (bytes)

T = System throughput (bytes per second)

n = number of vehicles in transmission range (number of messages received per beacon)

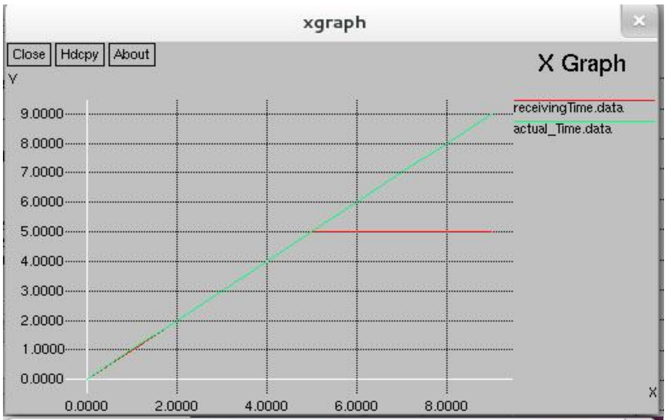
r = messaging rate (beacons per second) per vehicle

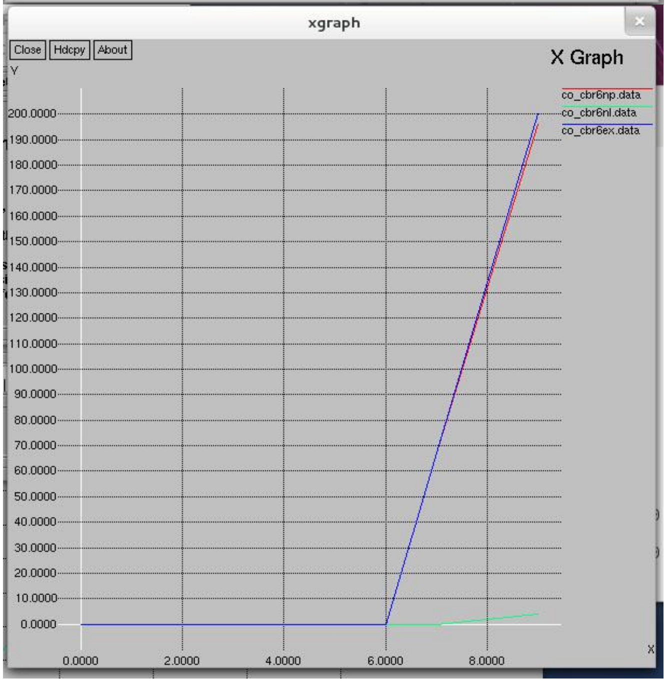
l = maximum allowable latency/beaconing interval (ms)

d = maximum tolerable processing delay per message (ms) In both scenarios, as explained vehicles are mobile and transmit DSRC messages every l ms over the communication range.

**Proposed Algorithm**
**Adaptive scheduling of message verification Algorithm**

```
DEFINE AC {AC3,AC2,AC0,AC1}
while (TRUE) do
    AC ← AC3;
    buffer Count ← 4;
    while (buffer Count>0) do
        buffer Count—;
        if (buffer [AC]! =null)AND (elapsedTime[AC]
            VERIFY messages from the beginning of buffer [AC];
        else if (buffer[AC]==null) then
            excessTime[AC]←maxDuration[AC]−elapsedTime [AC];
            for index = 0 to 3 do
                maxDuration[ACindex] ← maxDuration[ACindex] + pv index×excessTime[AC] P3 z=0 pvz ;
            end for
            AC ← NEXT AC;
        else if (elapsedTime[AC]>=maxDuration[AC]) then
            AC ← NEXT AC;
        end if
    end while
end while
```





The above fig shows the results shown by actual data and proposed data .the receiving data is our proposed technique Whose results are better than previous technique

## IV. CONCLUSION

Security is the major issue to implement the VANET. In this article we study the security requirements and challenges to implement the security measure in the VANET. Different types of attacks and their solutions are also discussed. We discuss some technologies

## REFERENCES

[1] Rashmi Raiya* , Shubham Gandhi "Survey of Various Security Techniques in VANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6, June 2014 ISSN: 2277 128X

[2] R. Saranya1, C. Yalini2, "A Survey on Secure Intelligent Transportation System Protocol for VANET using SMAP" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 10, October 2013).

[3] Vinh Hoa LA, Ana CAVALLI "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS : A SURVEY" International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[4] Gholamreza Vatanian Shanjani* and Somayyeh Jafarali Jassbi, "Taxonomy of Intelligent Transportation Systems (VANET): A Survey" Journal of Advances in Computer Research Quarterly ISSN: 2008-6148 Sari Branch, Islamic Azad University, Sari, I.R.Iran (Vol. 5, No. 1, February 2014), Pages: 69-82.

[5] Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3, "Security Analysis of Vehicular Ad Hoc Networks (VANET) " 2010 Second International Conference on Network Applications, Protocols and Services.

[6] Osama Abumansoor and Azzedine Boukerche, Senior "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012.

[7] Rasheed Hussain* and Heekuck Oh* "Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks" J Inf Process Syst, Vol.10, No.1, pp.103~118, March 2014

[8] Shamsul Jamel Elias, Mohd Nazri Bin Mohd Warip, R Badlishah Ahmad, Aznor Hanah Abdul Halim , "A Comparative Study of IEEE 802.11 Standards for Non-Safety Applications on Vehicular Ad Hoc Networks: A Congestion Control Perspective" Proceedings of the World Congress on Engineering and Computer Science 2014 Vol II WCECS 2014, 22-24 October, 2014, San Francisco, USA.

[9] Vimal Bibhu Kumar Roshan Dr. Kumar Balwant Singh Dr. Dhirendra Kumar Singh "Performance Analysis of Black Hole Attack in Vanet" I. J. Computer Network and Information Security, 2012, 11, 47-54

[10] TamilSelvan1, Komathy Subramanian2, Rajeswari Rajendiran3 "A Holistic Protocol for Secure Data Transmission in VANET" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, December 2013

### SHORT BIO DATA FOR THE AUTHORS

**Namarpreet kaur** She obtained her B.Tech (computer science & engineering) from Sai College of Engineering and Technology, Manawala, Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Security in Vanet

**Aman Arora is** working as an head of department in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. He obtained his B.Tech (computer science engineering) from Guru Nanak Dev University, Punjab, India, M.Tech (computer science & engineering from Guru Nanak Dev University, Punjab, India