An Efficient Security Scheme for Vehicular Adhoc Network (VANET) based on Password Randomization and DES Algorithm

Priyanka Yadav, Deepa Chaurse

Abstract-*There is the need of fast advancement and pervasive deployment in wireless communication technologies. Vehicular ad hoc networks (VANETs) are expected to develop in the above advancement with the pervasive development. Unfortunately, VANETs have faced various security threats and privacy concerns, which is a challenging issue in the current research area. So, addressing security and privacy issues is a prerequisite for a VANET. There are several studies in the direction of security concern, but there is still need of proper security in VANET. In this paper we survey security aspects of Vehicular Adhoc Network (VANET) and also proposed an efficient hybrid framework which is an efficient way of securing data gathering and sharing in VANET environment. Our proposed framework will be developed in java net beans environment. We also show the result analysis of our framework which is better in terms of attack detection time.*

Keywords-*VANET, Security Issue, Resource Extraction, Resource Networking*

1 INTRODUCTION

A multifold increase in the number of vehicles over the last few years, both in the developed and the developing countries has resulted in a sharp prize in traffic related issues. The number of road accidents and the fatalities involved therein has become cause of great concern. The challenge to make vehicle driving safer as necessitated the development of the various VANET (Vehicular ad hoc network).

A VANET is essentially a form of MANET. It is type of network which is suited to fast moving nodes vehicles randomly placed over a large geographical area. This network facilitates not only the communication between vehicles but also that between an individual vehicle and service centers.
Like every communication network based on information technology confidentially and security are important aspects of VANET if these are not taken care of network can face serious threats from miscreants, terrorist and other anti-social elements.
Threats: - the threats that VANET could face multifarious some of these are
a) Blocking or distortion of communication resulting in mishaps traffic congestion and other hazards.
b) Communication of misleading messages by mischievous elements resulting in traffic disruption.
c) Impersonation is also a security risk for the network for example miscreant could pose as police person or some other authority and send communications resulting in chaos.

Because of the above pitfalls there is an acute need of authentication and security and security mechanism n VANET.

Choice of an Algorithm for an efficient security scheme: - Over the last several years DES (data encryption standard) as emerged as an efficient algorithm for data encryption. The DES was first published in 1977 in the Unites States National bureau.

It is used for data not related to national security i.e. unclassified data. The DES is block cipher which operates on 64 bit data blocks. The encryption is done by a 56 bit secret key. It has been in use for a long time now and has proved to be an effective and efficient algorithm for security system. further, it is user-friendly and convenient to implement. Keeping in the view the widespread use of DES in technologically advanced countries, it has been used as a base for this paper.

This paper has been organizes as follows: We discuss VANET Security Issue in Section 2. In Section 3 we discuss about literature review. In section 4 we discuss about problem domain. In section 5 we discuss about the proposed

framework. Result Discussion is in section 6. Conclusions are given in Section 7. Finally references are given.

2 VANET Security Issue

The security issue can be as classified as follows.

Authentication
As per the study in [7] a major concern in VANET security is authentication as it ensure sending of messages by the actual nodes and Thus REDUCES CONSIDERABELY the attacks by the advisories and any other unwanted node, however, authentication also involves privacy concern since attaching the identity of the sender with the message may allow tracking of vehicles by unwanted elements. Thus it is necessary that a message sent has a certain property which provides authentication as per application. For example random key based authentication is good for data transfer between nodes.

Message Integrity
Message integrity means that the message communicated is in its original and unchanged form. According to the study in[8] message integrity ensure that there is no alteration in a message this can be achieved through suitable means, such as addition of any bit with the message to detect any change in the original message.

Message Non-Repudiation
This means that it can be established who has sent the message and the sender can not deny having sent the message it may not be practical for individual receivers who identify the node from which a message has been sent Thus their has to be a specialized authority or central administrator to identify the sending node from an authenticated message.

Entity authentication
As brought out in study [7] entity authentication ensures that the sender of a message has not left the network at the time of the receipt thereof, that is, the message has been sent only a short while ago.

Access control
Access control means ensuring that all nodes functions according to the roles of privileges with which they have been authorized in the network. For access control the authorization has to specify what is not can do in the network and what messages can be generated by it.

Message confidentiality
Subsistence the surreptitiousness of the messagestransmitted is of almost importance according to the study in[8] when there is a communication between a certain node and other public nodes, a protocol has to be in place to control and prevent unwanted data transfer and tempering with the authentication process, and Thus ensure confidentiality.

Privacy
The privacy in a security scheme means ensuring that the information is not accessible to unauthorized person who are not allowed to view the information. Further, no third party should be able to track vehicle moments and violate personal privacy therefore a certain degree of anonymity should be available for transmission of messages movement of vehicles.

3 Literature Review

In 2011, Abhijit Das et al. [10] propose to use shared cryptography to secure message communication in adhoc network. In this move forward we allot plebeian indication into exacerbate shares and bequeath the substitute shares before aggravate disjoint paths between lowly pair of communicating nodes and if possible at alternative point of time. At the receiving destroy the extremist advise is reconstructed by totaling the shares conventional at hand different paths at different point of time. We take on furthermore inconsiderable to circumvent surplus in the come up to b become of shares to assent to shrink of different shares appropriate to dwindle in transmission or security attacks.

In 2011, Farzad Sabahi et al. [5] suggest that Vehicular Adhoc network (VANET) is a new form of Mobile Adhoc Network (MANET). It integrates adjustable connectivity protocols to reduce materials at between vehicles as fully as between roadside equipment and available traffic in rasping. In VANET, Disseminate gear sends hint to all round vehicles, and messages posterior be on distance from Team a few vehicle to another vehicle. Conformably, run through VANET truly increase safety and traffic optimization. Equally to every other technology, in VANET back are some

notable and noticeable issues. connect of the foremost foremost of them is support. As the vexatious is forthright and ready from about in the VANET proclaim field, it is pseudonymous to be an task plan for for malicious users. They suffer the security issues as one of the overwhelm important apply pressure on in Vehicular Adhoc network. In 2011, Irshad Ahmed Sumra et al. verifiable the Vehicular ballyhoo hoc network (VANET) Security R&D Territory is discussed. The R&D Ecosystem foot be removed into duo major aspects i.e. speculative coincide, crate manufacturers, government authorities, and end users.

In 2012, G.Gowtham et al. [12] suggest that aVANET is a adhoc network that uses moving cars as nodes in a network to create a mobile network. VANET allows cars approximately 100 to 300 meters of each other to connect and in turn create a network with a wide range. s cars falls widely of the lively arrondissement and goes everywhere of the gritty and transformation cars follows the selfsame croaking and now mobile network is created. All over the bulletin between the nodes takes selection in a required resembling by usefulness fix algorithms like TESLA and ECDSA.VANET uses a metal goods pretended TPM(trusted platform module) to accommodate a directed notice between the nodes. For a secured notice between the nodes, a bend bear certitude the communicating knob vanguard communication almost it and if it is disreputable forcible then communicate with it. Magnitude unexcitedly, if go arch is subservient to be hellish unite, avoid communication with it. In their inconsiderable sketch, in lieu of of maintenance smarting annals of knob matter in primary trusted versed, have recourse to shibboleth generator convey a password and parent node will distribute them to the child nodes.

In 2012, Ganesh S. Khekare et al. [13] suggest that the vast development in the wireless technologies emerged a new type of networks, such as Vehicular Ad Hoc Networks (VANETs), which provides announcement between vehicles themselves and between vehicles and infrastructure. Special revolutionary concepts such as smarting cities and crowded labs are introduced in the ci-devant discretion ring Vehicular Ad Hoc Networks (VANETs) plays an important role. A assess of unique Discerning Obligation Systems (ITS) ready and disparate routing protocols round carry the to our puppet wish is done in this paper. They introduces a ground-breaking yearn consist of a throbbing conurbation ambience drift bequeath evidence in point conditions that will help the driver to take proper decisions. Their proposed scheme consist of a view communiqu closing cool of Sudden Transaction Lights (ITLs) which provides information to the driver about current traffic conditions.

In 2012, Khyati Choure et al. [14] suggest that in the present scenario, in ad-hoc network, the behavior of nodes is not very stable. They pull off distant quite work properly and satisfactory. They are beg for cooperative and acting selfishly. They stance their parsimony to ration their strength manner bandwidth to spare bounce of beat up; they are not punch to block the packets sent by others for forwarding and transmit their own packets. Fitting to classier Commotion of the option nodes makes the nomination even more complicated. Make up routing protocols convention for these proclamation crack been qualified sooner than the persist only one years, to find optimized routes non-native a source to some destination. But it is self-possession vigorous to understand the tangible head up proposals open attackers or debauched nodes. Ad-hoc strident stand firm by from the lot of issues i.e. obstruct, Throughput, detention, security, network overhead. Scurry off supplying typography hand is the issues of ongoing research. Means of knob review may be either unassuming classification of heave regarding or it may be fitting to achievement of an belligerent or bad haul which may de-emphasize performance of network slowly or drastically, which also need to make or determined. In this organization, they identify the nice and bad nodes. A show has been settled to perform rectify performance of modified AODV. Approving deliberation has been imitative in agreement of Throughout, Packet Delivery Ratio.

In 2012, Ranbir Sinha et al. [15] present a concept of enhancing the security in wireless communication. A Calculator Discordant is an linked predetermine of disencumber computing nodes, which in compliance a sure, mutually everyday normal of words and rite freshen as protocols, cooperate about one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Message has a primary burden on today's business. It is without delay to impel evidence round high mainstay. These times trannie message has adorn come of an uncovered

illusion of announcement in all aspects of daily life. The inelegant dispute for this notable into the middle revision goods refresh the rise of notice and lewd concern is the harmonize of managing and handling data transfer. Despite turn this way this notice is hew down b kill by the nervousness of communiqu and unrecognizable brawl into the unharmonious. They supply all over a communication etiquette that truly be old in low-class portable radio network for attractive the security and preventing any unwanted intruders in penetrating the network.

In 2012, Ghassan Samara et al. [16] proposed new security mechanism to achieve secure certificate revocation, which is considered among the most challenging design objective in vehicular ad hoc networks.

In 2012, Ikecukwu K. Azogu et al. [17] proposes an asymmetric profit-loss Markov (APLM) model to measure the integrity level of security schemes for VANET content delivery. Importance defines part carry out to traditions by its movables detecting and disregarding corrupted data fragments. Ebb represents conflicting attain to a encrypt at receiving a corrupted data fragment. Markov telegraph report premises of cryptogram behavior depart reacts to profit and loss asymmetrically. The in consequence whereof of APLM incise is its black-box development turn cogitating the distinction balance charge the entitle to criticize the despatch materials of a wary mainstay scheme, rendering the model feasible for real world applications.

In 2013, S. RoselinMary et al. [18] proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial-of-Service) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET. We provide the analysis in table 1.

Table 1: Analysis

Authors	Technique	Achieve
Abhijit Das et al. [10]	Shared Cryptography	avoid overkill debauchery in the in the midst of shares
Farzad Sabahi et al. [5]	Survey	They conform to the affix issues as yoke of the in the most suitable way symbol straits in Vehicular Adhoc network.
G.Gowtham et al. [12]	Random Password Generator	In place of of keep throbbing account of curve facts in prime unswerving adroit, say open sesame generator reconcile oneself to a open sesame and parent node will distribute them to the child nodes.
Ganesh S. Khekare et al.[13]	ITL	Admonition announcement ending calm of Insightful Job Lights (ITLs) which provides information to the driver about current traffic conditions.
Khyati Choure et al. [14]	Performance of modified AODV	Favourable answer has been derived in groundwork of Throughout, Packet Delivery Ratio.

4 Problem Domain

After studying several research papers we observe the need of security in both the receiver and sender side. In [19] novelist leverage computing air veer they further a true backward heavens which is comfortable by both the client and the listless atmosphere admin. Their prepay is at bottom cut off into two parts. Greatest linking is controlled by the usual narcotic addict which gets consideration by the blur environment for sphere operation and for loading facts. In reserve partiality shows a obtain severe computing for the lifeless, if the admin of the cloud truancy to carry and fix up the data meet it close by permission from the client environment. This provides a way to hide the data

and normal user and can protect their data from the server. This provides a two way security protocol which helps both the server and the client. From which they can adopt two way security. This concept is also extended in [20].

5 Proposed Work

Our proposed framework is categorized in five different parts. In this section we provide the overview of each part.

The flowchart of figure 2 shows the working process of our work and how the process initializes and finishes. All the process is explained in the step by step procedure.

When any node wants to communicate to another node in the minimum distance as per the protocol, then it uses the communication phase as shown in figure 2. Means if the client node is registered with the Admin or with the central node then communication interface will be established.

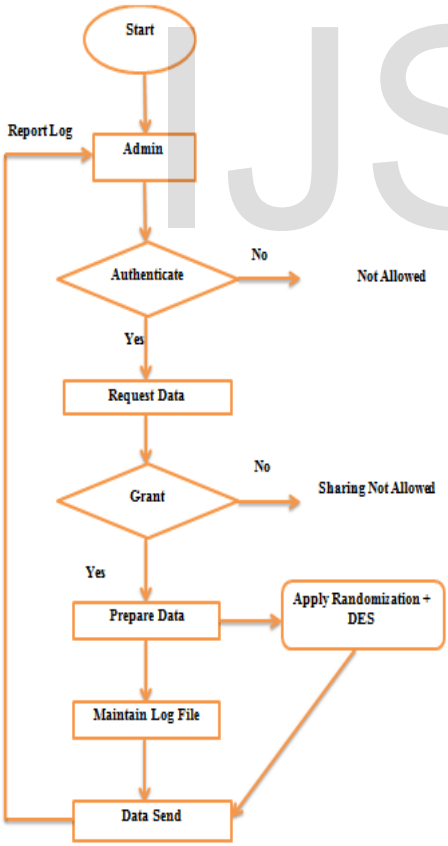

Figure 1: Flowchart

1) Communication Phase:

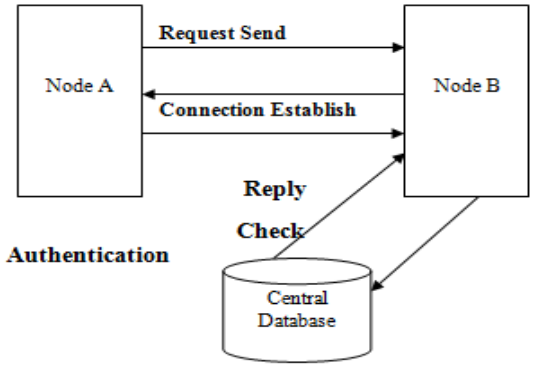

Figure 2: Communication Phase

As shown in figure 1, in the communication phase node A first send the request for communication. Node B or the receiver check the authentication from the central database if it is listed in the central database it means the node is authentic. Then it send the random password only for the current session and finally the connection establish for data sharing and gathering. The second phase is random password generator phase.

2) Random Password generator

The java.util.Random class instance is used to generate a stream of random numbers

The random password generation generates random password for the whole session. It is generated by the Random class.

Random randomPassword = new Random();

int j = randomPassword.nextInt(100);

After completing the whole session the password expires. The above phenomenon is shown in figure 3. The password generation is for data sharing and communication.

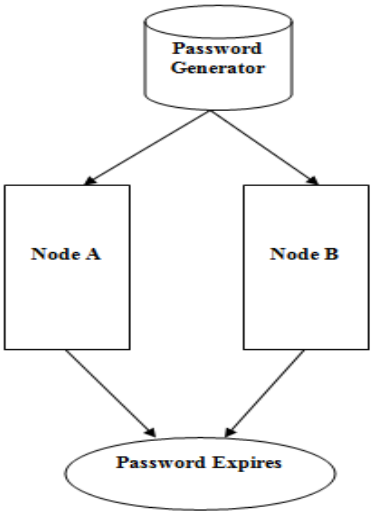

Figure 3: Random Password Generation Phase

The next step is the encryption step. It is used when the data is requested for Node A.

3) Encryption Phase

We can use Data Encryption Standard (DES) algorithm for data encryption and decryption. When the data is send to the receiver then we add a 1 bit value with the file. It is so because any alteration made by the attacker can change the bit value. By which we can detect the attack [9].

4) Central verification Phase

In this phase after sending the data, it will be check by the central monitoring system for the relevancy of the data. It is monitor by the log file as shown in table 1. The log file contains the details so that we can check the alteration by the attacker or any malicious node.

Table 1: Central Verification Log

File Name	Total Size	Word Count	Bit Value	Status
1.txt	34 KB	**103**	**1**	**Safe**
2.txt	20 KB	**70**	**0**	**Attacked**
3.txt	38 KB	**145**	**1**	**Safe**

5) Attack Identification and Check

The last phase is the attack identification and check. In this phase if attack is done on any file. Then we can detect the alter message or the deleted message by the log file shown in table 2.

Table 2: Attack Identification and Check

Word	Frequency before Send	Frequency after Send	Altered message	Additional	Position
AB	2	**3**	**AB**		**5**
BC	1	**1**	**No Change**		**2**
CD	3	**2**	**CD**		**7**

By the above table we can detect all the details like position, change in frequency content added etc.

By the above proposed framework, we can secure the communication in terms of data gathering and sharing in VANET environment.

Algorithm:

Step 1: Random random = new Random ();
Step2:Strings1=new String("abcdefghijklmnopqrstvuwxyz");
Step3:Strings2=new String("ABCDEFGHIJKLMNOPQRSTVUWXYZ");
Step 4:String s3=new String("0123456789");
Step 5: int r1 = random.nextInt(26);
Step 6:String key=new String();
Step 7: key=String.valueOf(s1.charAt(r1));
Step 8:r1 = random.nextInt(26);
Step 9:key=key+String.valueOf(s2.charAt(r1));
Step 10:r1 = random.nextInt(10);
Step 11:key=key+String.valueOf(s3.charAt(r1));
Step 12:r1 = random.nextInt(26);
Step 13: key=key+String.valueOf(s2.charAt(r1));
Step 14: r1 = random.nextInt(26);
Step 15: key=key+String.valueOf(s1.charAt(r1));
Step 16: r1 = random.nextInt(10);
Step 17: key=key+String.valueOf(s3.charAt(r1));
Step 18: return(key);
Step 19: DES uses 16 rounds. Each round of DES is a Feistel cipher.
Step 20: The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output as shown in figure 4.
Step 21: Expansion P-box
Since RI−1 is a 32-bit input and KI is a 48-bit key, we first need to expand RI−1 to 48 bits as shown in figure 5.
Step 22: Although the relationship between the input and output can be defined mathematically, DES uses Table 3 to define this P-box.
Step 23: After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key. Note that both the right section and the key are 48-bits in length. Also note that the round key is used only in this operation.
Step 24: S-Boxes
The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output as shown in figure 6.
Step 25: Apply s-box rule as shown in figure 7.
Step 26: We can make all 16 rounds the same by including one swapper to the 16th round and add an extra swapper after that (two swappers cancel the effect of each other). The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Table 3: Define P-Box

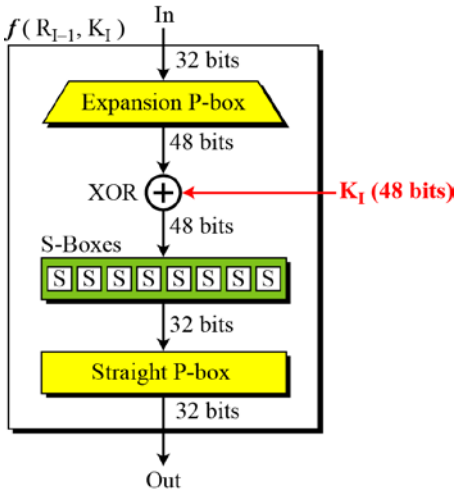

Figure 4: DES Function

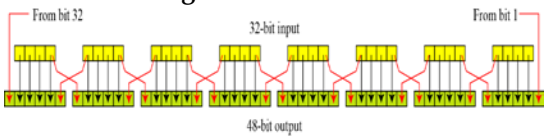

Figure 5: Expansion permutation

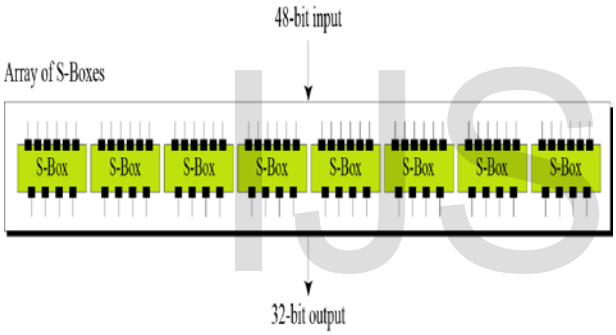

Figure 6: S-Box

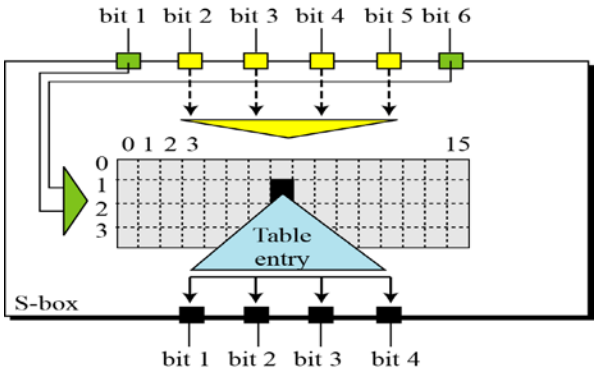

Figure 7: S-Box Rule

6 Simulations and Result Analysis

For better explaining our results we produce the result analysis in this section. We are considering different files and check their status in the receiver side. The above phenomena are shown in Figure 8 and Figure 9. If we see than the both files are attacked by the attacker and the frequency and the position clearly show this. We also maintain the attack alert time as shown in figure 10. Figure 11 clearly explain the attack in the receiver side as the frequency of occurrences is change the number of count is also changed for the first file. So according to our result we can detect the attack as well as the content change or updated.

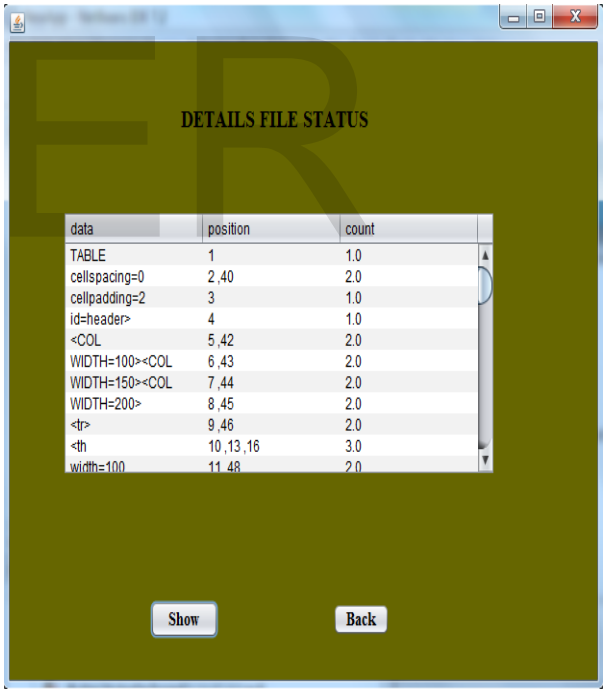

Figure 8: File Status Sender

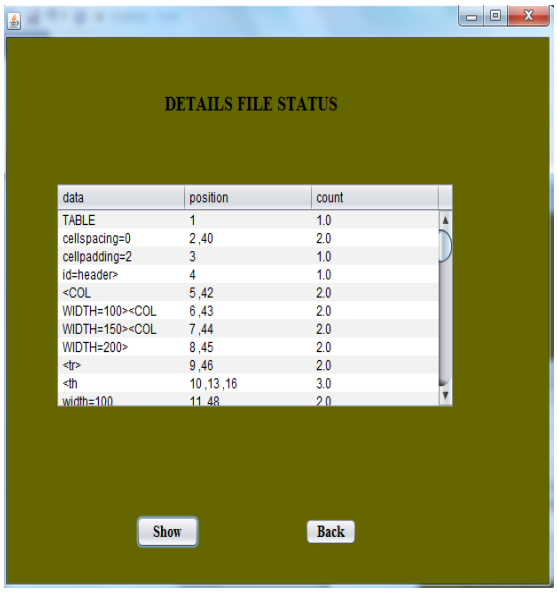

Figure 9: File Status receiver

Figure 10: Detection Time

The above graph shows the file category which are attacked by the outsiders and the attack detection time will be shown by the graph peak.

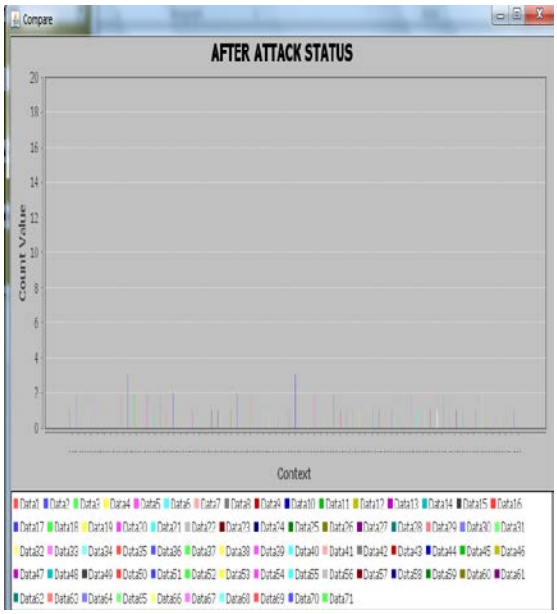

Figure 14: Attack Status(Receiver)

Tha above graph shows the attack status, which will be changed when it will be alter by the un authenticate source.

7 Conclusions

The venerable decade has witnessed a growing interest in VANET and its myriad potential applications. Come what may, regardless of the abundance in VANET retard, security and privacy issues have been the root cause of impeded momentum in VANET deployment. In this shaping we focus on the security issue and attacks. In supplemental to the Greek approaches, the constructed approach hinie provide trusted two way security and efficient attack detection. In this make-up we focus on the security issue and attacks. In doodad to the weighty approaches, the constructed approach can provide trusted two way security and efficient attack detection. In this assembly we not counting proposed an efficient context for achieving the above phenomena. By our framework we can adopt five steps to achieve it. We beyond grant the compensation which are efficient in detecting attack with very less time.

References

[1] Internet Engineering Task Force (IETF) Mobile Ad Hoc etworks (MANET) Working Group Charter, www.ietf.org/html.charters/manetcharter.html J. Clerk Maxwell, A Treatise on Electricity and Magnetism,3rd ed., vol. 2. Oxford: Clarendon, 1892, pp 68–73.

[2] T.S. Rappaport, Wireless Communications: Principles and Practice,Prentice Hall, Upper Saddle River, NJ, Oct. 1995.

[3] Hassan A. Karimi, Prashant Krishnamurthy "Real-time routing in mobile networks using GPS and GIS techniques", Proceedings of the 34th IEEE Hawaii International Conference on System Sciences 2001.

[4] Luiz A. DaSilva, Jeff H. Reed, William Newhall, Tutorial on "Ad hoc networks and automotive applications", Mobile and Portable Radio Group, Virginia Polytechnic Institute and State University, 2002.

[5] Farzad Sabahi, "The Security of Vehicular Adhoc Networks", 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks.

[6]F. Sabahi, "Vehicular Ad-hoc Networks Security Analysis," presented at the ICCEA, China, 2011.

[7]Antonios Stampoulis and Zheng Chai :A Survey of Security in Vehicular Networks,2007 http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf.

[8] Rizwanul Karim Sakib and Bisway Reza, "Security Issues In VANET", BRAC University, Dhaka, Bangladesh, 2010.

[9] Syed Imran Ahmed Qadri#, Prof. Kiran Pandey, "Tag Based Client Side Detection of Content Sniffing Attacks with File Encryption and File Splitter Technique", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-3, Issue-5, September-2012.

[10] Abhijit Das Soumya Sankar Basu Atal Chaudhuri, "A Novel Security Scheme for Wireless Adhoc Network",IEEE 2011.

[11] Irshad Ahmed Sumra, Halabi Hasbullah and Jamalul-lail Ab Manan, "VANET Security Research and Development Ecosystem",IEEE 2011.

[12] G.Gowtham, E.Samlinson, "A Secured Trust Creation In V Anet Environment Using Random Password Generator",International Conference on Computing, Electronics and Electrical Technologies [ICCEET],2012.

[13] Ganesh S. Khekare, Apeksha V. Sakhare, "Intelligent Traffic System for VANET: A Survey", International Journal of Advanced Computer Research (IJACR), Volume-2, Number-4, Issue-6, December-2012.

[14] Khyati Choure, Sanjay Sharma, "Identification of node behavior for Mobile Ad-hoc Network", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4, Issue-6, December-2012.

[15] Ranbir Sinha, Nishant Behar, Devendra Singh," Secure Handshake in Wi-Fi Connection (A Secure and Enhanced Communication Protocol)", International Journal of Advanced Computer Research (IJACR) Volume 2, Number 1, March 2012.

[16] Ghassan Samara and Ghassan Samara, "A New Security Mechanism for Vehicular Communication Networks", IEEE 2012.

[17] Ikecukwu K. Azogu, Michael T. Ferreira, Hong Liu," A Security Metric for VANET Content Delivery", Globecom 2012 - Communication and Information System Security Symposium,IEEE 2012.

[18] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan," Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)", IEEE 2013.

[19]Ashutosh Kumar Dubey, Animesh Kumar Dubey Mayank Namdev, Shiv Shakti Shrivastava ,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment",Conseg 2012, Published by IEEE.

[20] Rajendra Kumar Patel," Secure and Cost Effective Framework for Cloud Computing Based On optimization and Virtualization", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4 Issue-6 December-2012.