SECURITY PROVIDENCE FOR BATCH VERIFICATION SCHEME IN VANET BY USING PUBLIC KEY INFRASTRUCTURE FRAMEWORK

MPJ Santosh Kumar[1] & Dr. T. Anuradha[2]
[1]Research Scholar, Acharya Nagarjuna University
Assistant Professor, Dept. of Computer Science & Engg., GVP College of Engineering (A)
[2]Professor & Director, Dept. of Computer Science, JKC College(A)

Received: February 10, 2019 Accepted: March 14, 2019

ABSTRACT: *Data gathering is a big challenge problem in vehicular ad hoc networks (VANET). To overcome this problem, plenty of data gathering techniques have been proposed. None of the technique provides security in the process of gathering of data from vehicles to RSUs. The primary objective of this paper is to propose a secure as well as efficient data gathering technique that provides security and confidentiality to the gathering of data from vehicles to RSUs and vice versa. Performance of the data gathering technique proposed is evaluated by comparing the proposed technique with the existing data gathering techniques on the basis of message delivery ratio (MDR), average delay and computational overhead. Results of simulation assure that the data gathering technique proposed performs better in comparison to existing data gathering technique.*

I. INTRODUCTION

The Aim of Vehicular communication (VC) is to create a safer environment and better driving conditions for vehicles on the road. This happens through providing different types of applications; some are for the comfort driver and other for the safety of the driver. Safety applications are the most important and more urgent to develop, since it's matter of saving lives by preventing traffic accidents. The idea behind safety application in VC is to have a mechanism in which vehicles on a road can exchange data or information in a collaborative way to prevent accidents. This exchange of information is going to be through wireless messages between a vehicles and surrounding vehicles on the same road. The surrounding vehicle will use these messages to inform the driver of some dangerous situations happening on the road. Therefore, thorough these messages the driver of each vehicle will have more information that will help her/him to make a better decision regarding a specific situation.

Therefore, security and privacy are indispensable in vehicular communication for a successful acceptance and deployment of this technology, because attackersor pranksters can cause a huge *damage in terms of life and* road accidents as described in [12].

A prankster can for example inject false data and pretend that it's actually sent by a surrounding vehicle claiming that there is an accident ahead; this message injected to the network of communication can cause by itself accident and in some cases even pile ups.

Consequently, there is an acute need for securing the messages between vehicles on one hand, and authenticate each vehicle on the road on this other hand (vehicle should be known to be trusted). So, all vehicles on the road should be able to authenticate each other; however, another issue will rise in this case and might make the process of implementing VC harder. This issue is privacy, because each driver on the road should keep her/his privacy protected to accept to use this technology. Therefore, the authentication process should take place without affecting the privacy of the vehicles. Another issue that is raised is that it cannot guarantee that a previously honest node will not be corrupted in the future. For these reasons this project study proposes the use of Certification Revocation list (CRL), in which, the certificate authority will keep all the revoked certificates of vehicle, for a breach of trust, in this list. Consequently, all vehicles on the road should have access to the updated version of this list. For example, if a vehicle receives a message from a surrounding vehicle, it should check if that surrounding vehicle has a valid certification, otherwise the message received will be ignored.

In this study, the different proposed security mechanisms for VANETs, most of which haven't been implemented yet. Based on that study, compare these solutions, find and display the advantages and drawback, and finally proposed an optimum solution to that particular security issue addressed.

II. VANET INTRODUCTION

The idea behind VANET is to have a mechanism based on which nearby vehicles on the road can communicate in order to provide safety and comfort to the drivers and passengers. In order to achieve that, a special communication device will be placed at the level of vehicles willing to participate in the communication. Therefore, there is a need for V2V (vehicle to vehicle communication) common platform in order to achieve an accurate flow of data from node to node. This communication will allow building applications that are considered as safety applications, like emergency message dissemination, road condition warning and traffic incidents warning. The main objective of VANET communication is to provide a real time message dissemination platform to be used to exchange information between vehicles. Also, it should provide reliable exchange of information, which is used in entertainment applications like music sharing and gaming.

Therefore, implementing this technology will allow the driver to gather information about the road traffic which will be very useful for her/him to make life saving decisions on the one hand, and will provide to the driver and passenger some luxury applications like gaming with other passenger in other vehicles or even chat and socialize with the other passenger on the road.

III. ADVERSARIES, THREATS AND ATTACKS

As any wireless communication networkVANET is subject to many different kinds of attacks, which in some cases can be fatal. Therefore, it should be notice that any wireless device that runs on the same communication protocol stack can be a threat to the network.

The list of adversaries that should be aware of is very long, and the methods are very different.

Here are some types of adversaries:

Greedy Drivers [1]: are basically drivers who will try to convince the vehicle around her/him that there is a congested road ahead so that they will choose alternate routes and allow her/him a clear path to destination.

Snoops [1]: anyone nosy who wants to get a maximum information about other drivers around her/him including shopping habits, destinations. This information collected, can be used by spammers and probably harm the user.

Hackers or Pranksters: Teenagers or hackers probing for vulnerability and seeking fame.

Attackers: are the most dangerous adversaries to our systems, this will include individual or organized hackers.

Now exploring the most important vulnerabilities and its impact on VANET users. The first and simplest attack is when a malicious person send some signal that will infer and interrupt the wireless transmission between vehicles in the network, so that an attacker can easily and with limited transmission power, prevent communication in an area of the vehicular network as illustrated in the figure below.

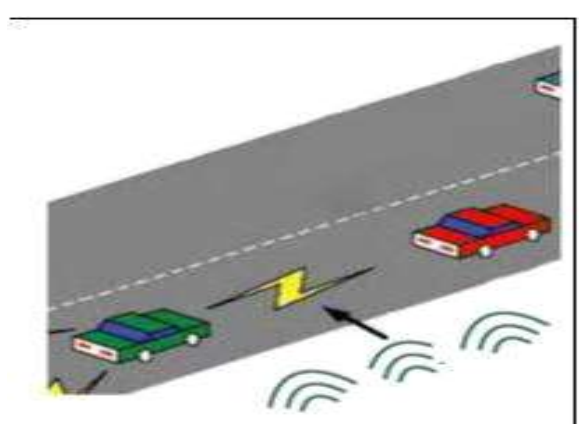


Figure 1: Illustration of signal interruption of V2V communication

Another threat that is very common in regular or wired attacks is spoofing, which basically means impersonating somebody you are not, and therefore, send messages to other nodes, which you are not supposed to send. So, combining spoofing with message fabrication can lead to very dangerous results. For

example, somebody who is not even on the road can disseminate a fake message of an accident, so everybody will more likely change their current route so there will make the load of vehicles unbalanced on the road which can create traffic congestions.

Or as mentioned above a greedy driver will use spoofing and pretend he/she is ambulance for example and have vehicles yield the road to him/her. Another threat is eavesdropping, so that an intruder will can interfere into the conversation of two drivers in two vehicles and get message in which there might be some important information critical to a driver's privacy, or will violate her/his privacy. Then using this private information, the hacker might be able to access the system of the target car and change parameter that can be crucial, like the speed of that car. This can lead to disastrous situation or even can be used in car hijacking.

Another common attack is DoS (Denial of Service) in which the attacker will overwhelm a vehicle or an infrastructure with messages in order to congest the channel. For example, a hacker will connect to a road infrastructure and pretend it's a vehicle on the road and start sending millions of message a second. That will lead the infrastructure to crash and therefore, there will be no V2I (Vehicle to infrastructure) communication.

The other form of attack that may face the VANET network is the suppression attack, it consists on a hacker connecting to the network and launching this attack by selectively deleting or dropping certain message. Of course this can cause a big damage, in case the hacker drops the message in which there is the accident warning, therefore, vehicle will be relying on the system to warn them, and since there is no warning, vehicles won't reduce their speed, which can lead to more accidents or in some cases pileups.

The last type of attack covered in this report is alteration attack mentioned in. It consists of attacking a network in order to alter the data inside the message exchanged on the road. The attacker will access the content of a certain message in the network and change it as wished. Again this can cause very serious consequences, in the case the hacker changes the message from a regular message to a warning which will affect the traffic on the road or even create incidents.

Of course not all attacks are covered here, but the ones that are most likely to happen in this type of network. But this doesn't prevent hackers from creating far more complex and innovative attacks on the network.

IV. CHALLENGES FACING IMPLEMENTING VANETs

VANET is a new and revolutionary concept that will change the way we think of roads and vehicles. However, implementing this technology will not be as easy as it looks. There are many challenges which prevent the implementation of such system.

The first problem deals with the law and identity disclosure in different countries and different cultures. Because for car companies to adopt the norms of VANET they need to make sure that this technology will appeal to the people of that certain region. Car to car communication will need some degree of authentication in order to secure the communication. Therefore, the authentication mechanism needs to have some degree of information about the vehicle and the driver, and this create concert for many drivers. It's totally understandable that most drivers on the road want their identity to be kept private, that's why this issue of privacy versus authentication, will be one of the main issues vis-à-vis implementing VANETs worldwide. To solve this issue VANET researchers thought of many solutions. One of the most reasonable ones was to use the car information instead of driver's information. That is, including the license plate information (number) of the vehicle, which actually constitute a unique id, in the authentication message that will be used in communicating with other vehicles.

The other main issue facing the implementation of VANETs on the road is availability. Meaning that all the system (Software and hardware) should be available to send receive message all the time, and in real time. For example, if a vehicle has an accident, it should send a warning messages to all the neighboring vehicles in real time or near real time so that the drivers of the other vehicles can avoid that accident, the figure below show how that works.

However, if there is a delay of broadcasting that message, the message will be meaningless since the other vehicles will not benefit from it.

Conversely, implementing a system whose response time is real time or near real time, will make it more vulnerable many different types of hackers' attacks, but DoS attack will have the most impact on the system. It will easily overwhelm the system with a huge number of meaningless messages and makes it crash easier. Hence while securing VANET need to take this problematic into consideration.

Another challenge for VANET is the range of coverage of the broadcasting a message. A message can be lost in the case of too few cars on the road, because there will be no vehicle to work as relay to that specific message and can be lost. Through some experiments conducted in [2] only 50% to 60% of vehicle on the

road will receive a message that was intended to be sent to them. This ratio is too low and poses questions on the effectiveness and efficiency of the system as a whole.

Another challenge is the error tolerance as mentioned in [1,3]. VANET is intended to reduce the number accidents and save lives. Therefore, the applications that should be used should have a very low rate of failure, otherwise, it can cause to disastrous results. Therefore, the applications to be deployed and used should have a very low margin of error in order for them to be deployed in vehicles.

Mobility is another concern to VANET developers, since vehicle network is so random and mobile. It's clear that the instability of the network will create the problem of the connectivity of the network, so that, if there is a few numbers of vehicles on the road, some of them will not receive the message, if this vehicle is outside the transmission range of the closest vehicle on the road.

Security Implementation requirements: The implementing security applications on a VANET ready vehicle can't be achieved without a regular maintenance of the equipment that VANET provides. Actually, a regular check on the software and hardware will allow the authorities (DMV in the case of America) to ensure that vehicle's software hasn't been changed or modified for the sake of impairing the VANET network on the road. As know inspection takes place in most of the countries worldwide once a year. An idea of inspecting VANET equipment more frequently (once in six months) would be very helpful in preventing hackers from modifying the purpose of the software embedded. This process will also help in updating certificates, and updating the 14 revocation list certificate. That is, download the latest updated list of vehicles whose certifications have been revoked for breach of VANET security regulations. It's very crucial that every vehicle using or holding VANET technology should be registered with an authority. It's very important to keep track of this technology users for statistics or logistic reasons, and the same time hold any driver accountable in case of discovering any illegal activity of the driver at the level of the network. A very important factor that makes securing VANETs communication possible is the fact that most of the drivers of the road are considered, or at least, most likely to be honest. Meaning that most of the users of the technology will attempt to modify or change the software or the configuration they are given. Therefore, most vehicles are most likely considered to act as it was intended at the conception level of the developers. Therefore, it is considered that most of the communication flow is not erroneous or injected by pranksters or hackers. However, this doesn't deny the fact of the possibility of having an unwanted or erroneous message flowing in the network. Fortunately, any hacker or prankster who want to attack or illegally access the network, has to be physically on the road, therefore, if there is a mechanism at the level of the victim vehicle to identify the attacker, and report it to the law enforcement, it will be easy for them to catch this person. Therefore, this will give an additional motivation to VANET applications developer to build applications that identify pranksters and repo.

V. RELATED WORK

An Expedite Message Authentication Protocol (EMAP) for VANETs, which exchanges the inefficient CRL check technique by an effective revocation checking process. Single-hop broadcast, multiple forwarding of packets, store the message in different RSU areas[14]. EMAP customs a profligate HMAC function and novel key circulation scheme paying probabilistic arbitrary key supply [1].

Based on decentralized CA, 2FLIP only needs numerous dangerous lightweight hashing methods and a fast MAC action for message signing and verification among vehicles [2]. EMAP can reduction the message damage percentage due to the message confirmation interruption associated with the predictable authentication approaches using CRL [3]. In addition, the RSU is able to autonomously prove the outputs since the verification function of the proxy vehicles [4]. To check the message validity at RSU, a batch verification of all signed messages is being performed by RSU, which is known as Identity-based batch verification (IBV) [5]. ID based signature scheme which consists of four algorithms namely setup, extract, sign and verify [6]. The other vehicles can also make the message authentication and identity verification based on the techniques of chameleon hash, HMAC and Diffie-Hellman key exchange [13]

VI. PRELIMINARIES

In the related work we discussed that if we doesn't send the proper information about the accidents done on the roads it will be very difficult to help the accident vehicles by the emergency vehicles. So the proper information should send to the near vehicles, so by sending the proper information to the near vehicles it will be very easy to the emergency vehicles to help the accident vehicles.

To send the perfect information to the near vehicles by using the public key infrastructure algorithm.

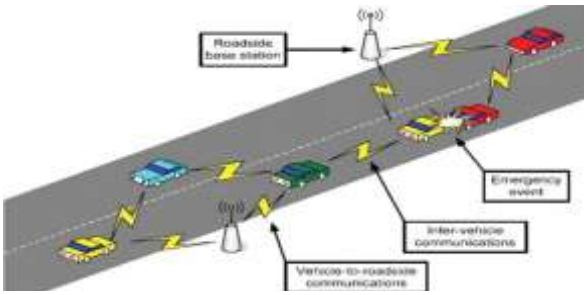


Figure 2: V2V and V2I in the case of an accident on the road

So from the above figure say that if it is send the proper information about the accident to the near vehicles can easily give way to the emergency vehicles.

VII. PUBLIC KEY CRYPTOGRAPHY AND RSAALGORITHM

1. Choose two large prime numbers p and q randomly
2. Let n = pq.
3. Let $\phi(n) = (p - 1)(q - 1)$.
4. Choose a large number e ϵ [2,ϕ-1] that is co-prime to $\phi(n)$
5. Compute d [2, ϕ-1] such that ed modϕ (n) = 1 or ed = k× $\phi(n)$+1
   There is a unique such d. Furthermore, d must be
   co-prime to $\phi(n)$
6. Announce to the whole word the pair (e; n), which is his public key
7. Keep the pair (d; n) secret to himself, which is his private key
8. Sender will now use the public key to encrypt the message M as follows
   $C = M^e \bmod n$. Here, C is the encrypted message.
9. Receiver will use its own private key to decrypt the message by using the equation.
10. $M=C^d \bmod n$

RSA EXAMPLE:

i. Select primes: p, q, p ≠ q p = 17, q = 11
ii. Compute n = p×q = 17×11 = 187
iii. Compute $\Phi(n) = (p-1)(q-1) = 16x10 = 160$
iv. Select e, such that gcd(e,160) = 1; $0 < e < \Phi$ say, e = 7
v. Determine d: de=1 mod 160 and d<160 value is d=23 since 23x7= 161 = 10x160+1
vi. Publish Public Key KU = {7,187}
vii. Keep Secret Private Key KR = {23,187}
viii. RSA Encryption/Decryption is M = 88 note that 88<187
ix. Encryption is $C = 88^7 \bmod 187 = 11$
x. Decryption is $M = 11^{23} \bmod 187 = 88$

VIII. PROPOSED SYSTEM

Proposed scheme enhances the features of IBV scheme for VANET, such as recognizing illegal signatures. If attackers send some invalid messages, the batch verification may lose its efficiency. This problem can be solved by using public key algorithm based on PKI (public key infrastructure) technique.

IX. PROPOSED SECURITY SOLUTIONS

To successfully deploy VANET on roads, need to face the problem of potential security threats presented above. To do that, they were many attempts in different papers to address these issue. Some of these attempts were worth considering and cited in this section.

- ***Authentication and location detection***

The first issue that the need to address is making sure that the message is really sent from the party that pretends to send it. Therefore, there is a need of using authentication of all vehicles on the road.
In the paper [1], the authors introduced the concept of authenticated localization of message origin. This approach is intended to prevent any person sitting on the edge of the road from pretending that his message

originated from a vehicle travelling on the road. Therefore, this will prevent spoofing, in which, pranksters fake their identity to pretend that they are vehicles on the road in order to disturb the order of the traffic.
To do this, each vehicle should be kept track of by some authority or infrastructure in some cases, by using authentication. To achieve this public key cryptography authentication is used. In this fashion, each vehicle will broadcast its identity (public key) along with the signature of a current timestamp. This is very important to make sure that the authentication is recent and at the same time have different signatures from the vehicle to ensure its identity.
So when each vehicle receives such a broadcast, it signs the other vehicle's ID and rebroadcasts it. Doing this will help vehicles to predict the location of the specific vehicle on the road. For example, if a vehicle A receives a public key of B Kb, it adds its signature {Kb}ka with its private key Ka to its regular broadcast. Therefore, if vehicle B hears C rebroadcast A's identity, before rebroadcasting B's identity, then it knows that A is ahead of him. Further, a vehicle B can get more assurance that vehicle A is ahead of it by getting rebroadcasts of A's identity by vehicles D and E [1]

- ***Preserving Privacy and Anonymization***

In VANETs the issue of privacy and preserving the personal information of a driver and vehicle, is raising concerns for both car manufacturers and future potential users. Therefore, there shouldn't be any disclosure on any private information of the driver or vehicles. So a vehicle should not trace the exact identity of other vehicles of the road, but only to verify the connection between the information sent and the vehicle present in the road. In other words, make sure the vehicle it pretends to send the message, is indeed the one who really did.
To achieve this, there is a need to include an intermediary service that will map the permanent identity of the driver or/and vehicle and a temporary ID. The authors called this service, anonymization service first introduced by [1]. This service as mentioned earlier maps between the permanent identity of driver or vehicle and a random ID it provides to that vehicle to keep track of it; it's extremely important that this temporary ID should not be traceable to the driver or vehicle. Therefore, there should be a strong algorithm at the level of the anonymization service to achieve that.
Although this technique will create an additional overhead, it will provide the driver with the required privacy and prevent spoofing.
Anonymizers should be placed on a toll booth then there will be re-anonymizers on the side of the road on a regular distance difference between them.
So when the vehicles approach a re-anonymizer as proposed by [1], this latter would broadcast a random nonce N, then the vehicle will sign N, and broadcast the new certificate encrypted with the old public key.
Then, the re-anonymizer will verify the signature and broadcast the new certificate encrypted with the old public key, after that, it will verify the signature and broadcast the new certificate encrypted with the old public key. The certificate contains the new identity of the vehicle and a timestamp as well as the re-anonymizer signature. Consequently, every time a vehicle will approach a re-anonymizer, it will acquire a new identity, for added security.

- ***Secure Aggregation technique***

Using this technique, each vehicle on the road will keep count of the vehicles it passesand authenticate them. Authentication will take place using an infrastructure aid that will deliver as explained above some unique valid IDs that can be understood by all vehicles on the road, and as mentioned above will preserve the privacy, as described in [6,7]
Through this information collected each vehicle will have an estimation of the number of vehicles ahead.

- ***Active Position Detection***

-

Position security in VANET is very important to the process of verifying the source of any communication or message through the network. To achieve that, need to use on-board radars to detect neighboring vehicles and to confirm their coordinates. Based on that data, a history of the vehicles movement is created. Consequently, a check on the history and computing similarity, this can prevent a large number of Sybil attacks and position based attacks, described in details in [3]

X. PUBLIC KEY INFRASTRUCTURE INSIGHT

What is PKI?

At the basic level, PKI (Public Key Infrastructure) can be described as a technique that enables users on a

network to securely exchange data. This is achieved by the use of public key/ private key pair, that are generated and exchanged through a certified authority. A PKI is an arrangement that binds public keys with user's identities through a certificate authority (CA).

CA uniquely identifies user identities individually. To achieve that, each user must be individually registered with a CA. After registration the CA adds this user to a list and updates its list of user's identities and their assigned public keys. In addition to the registered users, CA will keep another list of the users with revoked certification.

Meaning, the ones who were registered before, and for a reason, they should not trust anymore.

Why Use PKI*:*

PKI is used because it assumes the use of *public key cryptography*, which is the most common method on the Internet for authenticating a message sender or encrypting a message.

It has an advantage over the creation of a shared for encryption and decryption of data. The traditional shared key can be stolen by a hacker or an intruder in the middle, and then this person will be able to decrypt the secret data using the shared key he/she could have. Using PKI prevents this, since both parties have different public keys.

- ***Advantages of PKI over other encryption techniques:***

PKI allows two network users to authenticate each other to exchange encrypted data without prior contact. Therefore, there is no password exchange needed, which can be very dangerous in almost every medium. Since nobody can guarantee that a network is completely secure.

Another advantage for PKI infrastructure is the smooth and easy logic behind the PKI infrastructure: To sign a message, the sender encrypts a message with his private key. The receiver decrypts with the public key of the sender and if the 'message' is what is expected then the receiver knows that it can only be send by the sender.

- To encrypt something the sender encrypts the message with the public key of the receiver. Then only the receiver can decrypt the message using his private key.

XI. SIMULATION AND RESULTS

In this simulation I mainly tried to work on implementing the solution proposed in this study for securing VANET communication. I worked on an applet in which V2I (vehicle to Infrastructure) communication is illustrated. In this applet, there are two types of vehicles; regular vehicles, which are the vehicles that do not have transmission capabilities, shown in yellow in the applet, and the smart vehicles which have the ability to communicate with the infrastructure. The infrastructure used here are the traffic light which should be changed whenever there is a smart car coming down the road.

The work mainly consisted in computing the response time in the communication between a smart vehicle and the infrastructure. The response time is measured in case there is the use of PKI encryption technique and without it.

These measurements are meant to check the feasibility of implementing such encryption technique in the case of V2I (Vehicle to Infrastructure) communication.

These measurements are done through Eclipse Java simulator and in a limited capabilityenvironment processor (mobile device processors) that emulates the processor for a regular VANET equipped vehicle capable of transmitting and receiving messages.

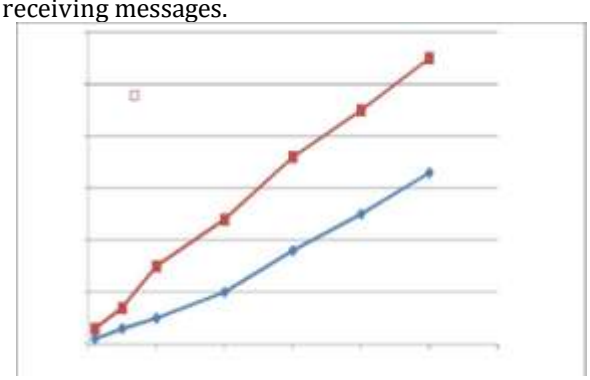


Figure 3: Response time Simulation Results

Response time without encryption

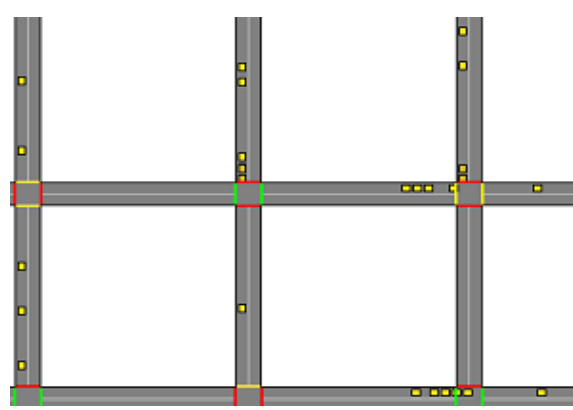
Response time with encryption

Figure 3 shows the response time of VANET ready vehicle, in the presence and the absence of PKI encryption. The results obviously show that the response time in the case of encrypted communication is higher than in the regular communication (without encryption)
And this result was as expected in the theoretical analysis of this problem, since there sure will be an overhead, as mentioned earlier in the report, due to handling public and private keys, signing etc.
Another observation is that the more the density in the road there is, the more the response time is greater. Again, this result was expected in the theoretical phase due to the queuing mechanism at the level of the infrastructure. There will be a delay in handling all messages from all vehicles.

XII. IMPLEMENTATION

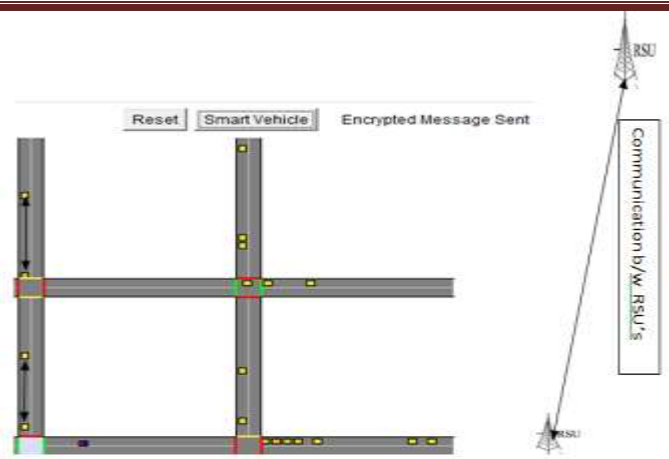
The implementing security applications on a VANET ready vehicle can't be achieved without a regular maintenance of the equipment that VANET provides. Actually, a regular check on the software and hardware will allow the authorities (DMV in the case of America) to ensure that vehicle's software hasn't been changed or modified for the sake of impairing the VANET network on the road. As itknows inspection takes place in most of the countries worldwide once a year. An idea of inspecting VANET equipment more frequently (once in six months) would be very helpful in preventing hackers from modifying the purpose of the software embedded. This process will also help in updating Certificates and updating the14 revocation list certificate. That is, download the latest updated list of vehicles whose certifications have been revoked for breach of VANET security regulations. It's very crucial that every vehicle using or holding VANET technology should be registered with an authority. It's very important to keep track of this technology users for statistics or logistic reasons, and the same time hold any driver accountable in case of discovering any illegal activity of the driver at the level of the network. A very important factor that makes securing VANETs communication possible is the fact that most of the drivers of the road are considered, or at least, most likely to be honest. Meaning that most of the users of the technology will attempt to modify or change the software or the configuration they are given. Therefore, most vehicles are most likely considered to act as it was intended at the conception level of the developers. Therefore, it is considered that most of the communication flow is not erroneous or injected by pranksters or hackers. However, this doesn't deny the fact of the possibility of having an unwanted or erroneous message flowing in the network. Fortunately, any hacker or prankster who want to attack or illegally access the network, has to be physically on the road, therefore, if there is a mechanism at the level of the victim vehicle to identify the attacker, and report it to the law enforcement, it will be easy for them to catch this person. Therefore, this will give an additional motivation to VANET applications developer to build applications that identify pranksters and report them. A similar approach was mentioned in [4]. This will really make the task of hacking riskier for pranksters or hackers, compared to regular wired networks.

XIII. RESULTS



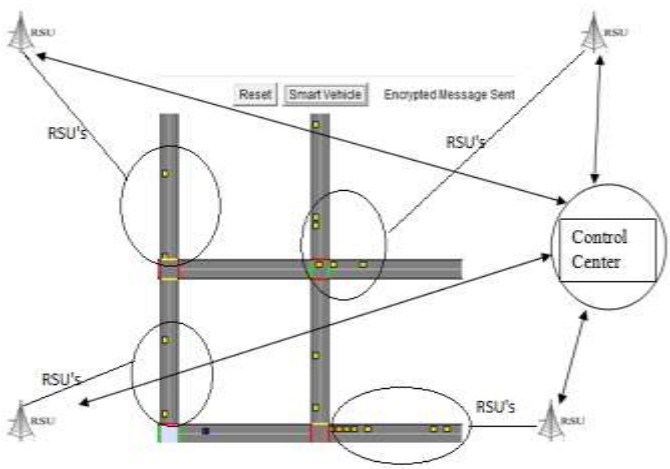
Java simulation Before smart vehicle

From the above diagram we can say that here the admin is monitoring the vehicles and in the diagram we also have signals by those signals the vehicles may move in the correct direction. Here the vehicles are moving in the all four directions.



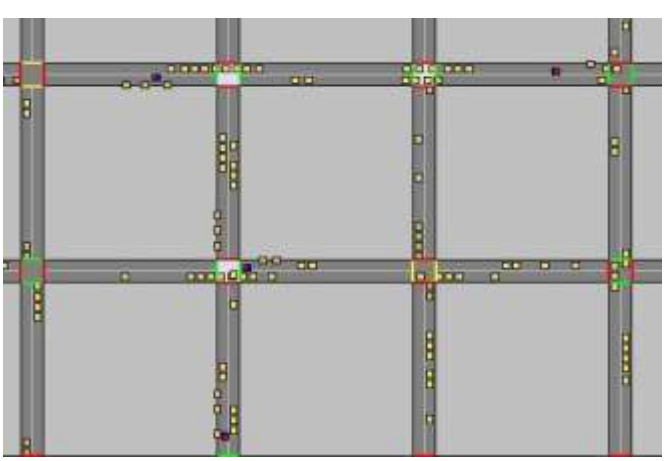
Java applet simulation when encrypted message send

Here in the above diagram the communication takes place b/w RSU's to RSU's. The vehicles can get the information from the RSU's and vehicles communication is passing through RSU's and to get the smart vehicle in the way of the general vehicles.



Java applet simulation and communication b/w RSU's and vehicles

Here in the above diagram the simulation is done. The communication takesplace in the vehicles and RSU's and vice versa. By sending the correct information to the general vehicles those vehicles communicate with smart vehicles and give way to smart vehicle. From above diagram says that here the encrypted message of the smart vehicles has been send to the normal vehicles.



Java Applet Simulation after entering smart vehicle

In this simulation I mainly tried to work on implementing the solution proposed in this study for securing VANET communication. I worked on an applet in which V2I (vehicle to Infrastructure) communication is illustrated. In this applet, there are two types of vehicles; regular vehicles, which are the vehicles that do not have transmission capabilities, shown in yellow in the applet, and the smart vehicles which have the ability to communicate with the infrastructure. The infrastructure used here are the traffic light which should be changed whenever there is a smart car coming down the road.

XIV. CONCLUSION

Securing VANETs communication is a crucial and serious issue, since failure to do so will delay the deployment of this technology on the road. All vehicles' drivers want to make sure that their identity is preserved while exchanging messages with the other entities on the road. On the other hand, the governments want to guarantee that the deployment of such system will not cause more accidents due to security flows. In this study I tried to focus on the real issues facing the VANET security and tried to select appropriate solutions to face most of the security issues is presented. Finally, I tested a feasibility of introducing PKI to VANET communications and encouraging results in the case of V2I communications. V2Vsecure communication hasn't been simulated in this study and should be further investigated and simulated using NS2 or other simulators.

ACKNOWLEDGEMENT

I would like to thank Dr. T. Anuradha, and the anonymous referees for providing valuable comments and suggestions on this paper.

REFERENCES

1. A.Nandini,P.VenkateshwaraRao "Broadcasting message Authentication protocol for Vehicular Ad Hoc Networks using Cluster Technique"IJAEGT ,Volume 2,Issue 09,September,2014.
2. FeiWang,Student Member "2FLIP: A Two –Factor Lightweight PrivacyPreserving Authentication Scheme forVANET"IEEE,yongiunXu,HanwenZhang, Zhu,2015.
3. A.M.Suhavaneswari,A.Muthukrishnan "A Cluster Based Expedite message Authentication Protocol For VANETs"(IJARSE) International Journal of Advanced research In Science and Engineering ,Vol-3,Issue No.4,April 2014,ISSN-2319-8354(E).
4. YiliangLiu,LiangminWang,Hsiao-HwaChen,Fellow "Message authentication using proxy vehicles in Vehicular Ad Hoc Network",Member,IEEE,Vol-64,No-8,August 2015.
5. PratabidyaMahapatra,A.Naveena "A Survey on Identity Based Batch Verification Scheme For Privacy and security in VANET",Vol.3,Issue No.04,April 2016.
6. Y.Bevishjinila, K.Komathy"An Efficient Authentication Scheme For VANET Using ChaCheon's ID Based Signatures" Computer Science, Volume 4,Issue No.6,June 2014,ISSN-2249-555X.
7. ShahnawajKhan,NaveenChauhan "Region Authority Collaborated Certificate Organization and Management in VANET"The Third International Conference on Advances in Vehicular Systems,Technology and Applications,Vehicular 2014.
8. R.Rajan,S.Narendran,M.Prasanth,R.Rajkumar"Hybrid Message authentication Protocol In VANET" Computer Science And Information Technologies, Vol.5,Issue 2,2014,1696-1697,ISSN:0975-9646.
9. ChenxiZhang,Pin-Han Ho "An Efficient Message Authentication Scheme for vehicular Communications" IEEE,Transaction on Vehicular Technology,Vol.57,No. 6,November 2008.
10. VinhhoaLA,AnaCAVALLI" Security Attacks and Solutions in vehicular Ad Hoc Networks: A Survey" international journal on Ad Hoc Networking Systems(IJANS) Vol. 4,No 2,April 2014.
11. Nitish Kumar Bharti,Manoj Sindhwani" Enhancing The Massage Authentication Process in VANET Under High Traffic Condition Using The PBAS Approach" Indian Journal of Science and Technology,Vol.9(47),ISSN(Print):0974-6846,DOI:10.17485/ijst/2016/v9i47/106794,December 2016.
12. Godavari H.Kudlikar,Sunita S.Barve"Proxy based Batch authentication Scheme For Vehicular Ad-Hoc Network" International Journal Of Computer Science trends and Technology (IJCST)-Volume 4,Issue 3,May-June 2016.