Enhancing Security in VANET in terms of Confidentiality and Authentication

Opinder Kumar
Computer Science and Engineering
Lovely Professional university
Punjab, India

Mohinder Kumar
Computer Science and Engineering
Lovely Professional university
Punjab, India

ABSTRACT

VANET is very useful for solving traffic related problems and provide safety to life's of Drivers and passengers moving on the road, In this paper the proposed algorithm is helpful in authenticating a user and Solving Traffic related problems and provide more efficient broadcast system by covering Large distance. According to this Approach Vehicles can communicate with RSU,but there is no Vehicle to vehicle Communication. RSU can communicate with each other and update their information to the nearest RSU (NRSU), after that the emergency broadcast is also done by the NRSU. For security reasons we consider Vehicle numbers as their pseudonym and apply a new approach to authenticate the user, So that no unauthorized user can broadcast and send any false information to RSU. The public Key Cryptography is used to encrypt the communication between Vehicles and RSU.

Keywords
VANET, Authentication, encryption, RSU, NRSU, Driver License number, password, Vehicle number

1. INTRODUCTION

VANET have received a great attention due to the promises made in the intelligent transportation Systems. In VANET vehicles are equipped with sensors and wireless communication devices to sense the road traffic and sent alert messages to nearby Vehicles and send information to RSU. In VANET vehicles (OBU) can communicate with the vehicles within their range and also can communicate with RSU. When any accident takes place the other vehicles passing by accident site observe that event and send alert messages to RSU and the other vehicles within their range. RSU receives so many alert message, first RSU checks the location id where the accident happened, if it is not present in the previous alert messages it counterchecks for the messages and verify the user, if the location is not present and user is authorized then RSU generate an Emergency broadcast messages about the accident and its location, So that vehicles coming on that road may not lead to accident, if the message is already broadcasted the new messages for the same location are not considered by the RSU. So VANET is helpful in preventing accidents and Road traffic related problems.

In this paper we propose a new method to verify the user and also perform public key cryptography to encrypt the communication between the user and the RSU so that no private information about the user can be accessed by anyone else. Our proposed algorithm has a broadcast method that is capable to cover long distance and makes VANET more efficient in preventing accidents and authenticates users. This approach not only deals with the security issues but also with the road safety challenges like broadcast storm, Building Shadow and intersection problem. Now we present the graphical representation of the scenario taken in this algorithm for VANET

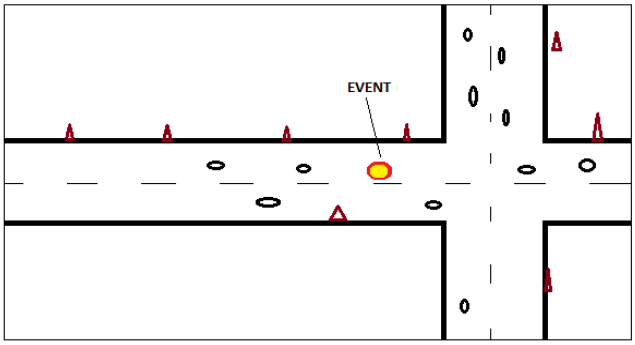


Figure 1. Event showing accident spot

Fig.1 shows the road map for a city, RSUs are installed at the distance of 1000 meter and some critical points distance can be reduced, these critical points include areas like railway crossing, over-bridges, under-tunnels etc. The highlighted area on the road shows a place where event (accident) has occurred. In Fig2. Some vehicles observe the event and sent an alert message to RSU. In Fig. 3 after counter checking the information RSU will send broadcast message to all the vehicles in its area and also to MA and NRSU and MA will update the alert message in the whole city to prevent accidents and traffic problem.

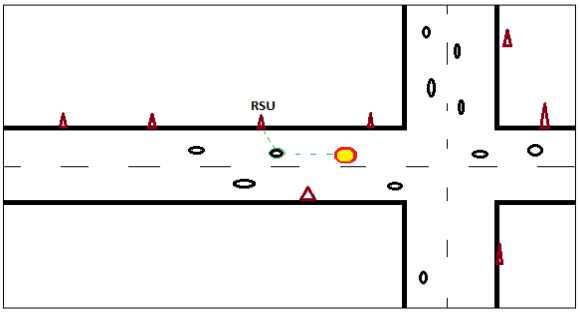


Figure 2: vehicle sends message to broadcast

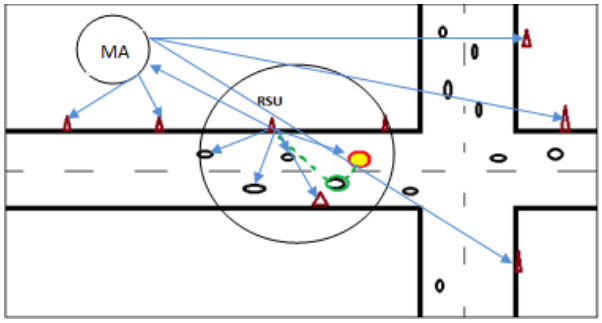


Figure 3: message broadcast from MA & RSU

2. RELATED WORK

There are so many security protocols in VANET which aims at privacy preserving authentication, these protocols have been developed on the basis of Digital Signatures, group signature, and location based keys and anonymous certificates using pseudonyms of vehicles to conceal the real identity of the user. Y. Park. K-H Rhee of Pukyong National University have proposed a pseudonym-based privacy preserving authentication and a hierarchical identity based cryptographic scheme for location aware services, RSU issues vehicles location based Keys for location aware services and MA is an authority that is in charge of registering RSUs and vehicles deployed on a VANET, MA issues cryptographic materials through initial Registration[1].

Shou- Chih Lo.Chih Cheng Tseng have proposed an efficient broadcast scheme that is based on water wave propagation to spread alert messages and solve problems like connection hole, building Shadow, Intersection problem. Carry and Forward mechanism is used to propagate messages [2]. M. Raya and J. P. Hubauxhave proposed some building blocks for secure vehicular communication including anonymous message authentication by using digital signatures [3].

Y. Park. K-H Rhee of Pukyong National University have proposed an efficient authentication protocol with anonymous public key certificates for secure vehicular communications [4]. Kanitsorn Suriyapaiboonwattana, Goutam Chakrabortyhave proposed APAL broadcast protocol Adaptive Probability Alert Protocol is another such technique which uses probability technique to rebroadcast the message. This algorithm does not need location information of any vehicle. In this algorithm, upon receiving the message for the first time the receiver waits for a random time given by Δt.

After the expiry of the random time interval it will check whether it has received same alert packet from some other node or not, if yes it discards the packet otherwise it rebroadcast with high probability. Process repeats up to certain upper limit of duplications that can be handled by the single node.

Count time = $\Sigma i \Delta t$

If condition is true the nodes will continue to propagate messages else exit the process [5].

(srivastava, 2013) have proposed All Unit Interconnection Algorithm which is helpful in solving the connection hole, building shadow, message storming problems to great extent by using a conditional broadcast algorithm

In this paper, our proposed Algorithm is helpful in authenticating a user and provides a much better broadcast system that covers a long distance and VANET broadcast become more efficient. There are certain assumptions that have been made which will be discussed later in this paper.

Here we list the notations that will be used in the algorithm.

- Drivers License Number
- Car Number
- Passwords
- Road side Units (RSU)
- MA

3. ASSUMPTIONS

There are some assumptions that are made for developing the algorithm.

1. RSU is available at every traffic signal and intersection road and also in critical sections.
2. Critical section includes areas like railway crossing, over-bridges, under-tunnels etc.
3. Every vehicle on the road is equipped of GPS system and has an interface to input Driver License Number, Password, and an inbuilt system that shows the vehicle number.
4. Range of RSU is 1000 meter.
5. Vehicles are not allowed to communicate with each other (No V2V).
6. User doesn't share their password or private Key with anybody else.

4. ALGORITHM

The proposed algorithm is

1. Start()
   {
   a. For authentication car drivers presents its License number, Password to the Road side Unit.

b. The RSU unit verifies the Car number, Drivers License number and password.
IF (Send information = stored information)
{
a. RSU send message to car for successful authentication.
b. When car receives the successful authentication message ,car will start

}

Else

{

a. The RSU unit sends unsuccessful authentication message to the car.
b. Again car will send its credentials to the RSU again authentication procedure will be repeated
IF (un-successful authentication>=threshold value)
{
a. Car will be blocked for the certain period of time

}

Else

{

a. Successful authentication will be done and car will start communication
b. The communication between the smart cars is encrypted and decrypted by using public and Private Key cryptography.

}

2. When accident happen
   Start ()
   {
   a. The successfully authenticated car will send message about accident to the RSU.
   b. RSU send message to MA.
   c. MA will broadcast the accident information throughout the city.
   d. When cars receives the information who are on the same road where accident happen ,it will change its path

   IF (Path exits)
   {
   a. Car will change its path

   }

   Else

   {

   Car will wait unless road will be cleared

   }

End of algorithm

5. ALGORITHM EVALUATION

In this section, the performance of this algorithm is discussed that it can perform. First of all user have to authenticate itself to access the services of VANET. After this vehicles are allowed to access the services of VANET. All the communication between vehicles and RSU is encrypted by using public and private key cryptography. There is no vehicle to vehicle communication allowed, So message storming problem is solved, If any accident occurs, the vehicles by the site send RSU an alert message, RSU counter checks the validity of the user, if user is valid then RSU update their information to MA and the vehicles within its range. MA will broadcast this message to all the RSUs in that location or city, So that accident can be prevented and traffic problem can be solved easily by mentioning a new route instead of that road where accident occurs, if there is no sub route available traffic have to wait till the road is cleared.

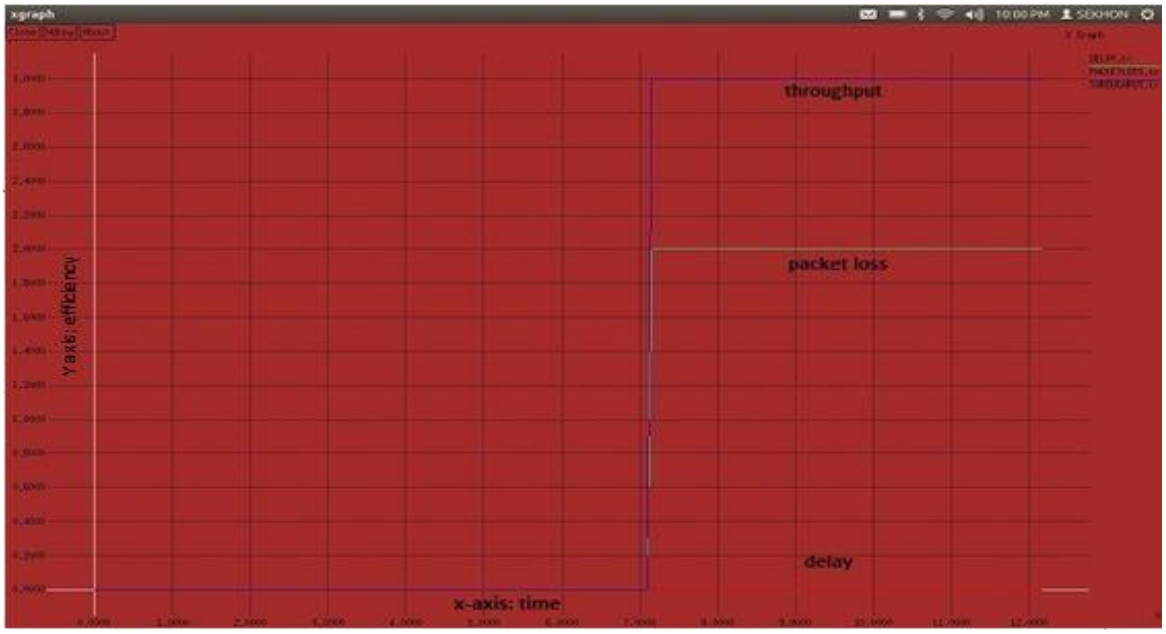
1. User provide information to RSU which includes Vehicle number, Users License Number & password, if the information provided by user is correct then the vehicle starts and can access information from RSU and also send information to user. If information provided by user is invalid then he\she is given a chance, if information is wrong again the car is blocked for a certain period of time. The car will start and access the services provided by the network.
2. If accident takes place, it is observed by the vehicles that are moving on the same spot, The vehicle that observe the accident will send the information to RSU, RSU will check the information, if it is send by a valid user, this information is broadcasted in its area and also information is updated to MA, MA will broadcast the information to all the NRSU within the respective areas. The whole communication between RSU and Vehicles is encrypted with public and private Key cryptography.
3. When the cars on that route received the information they will change their Route to a sub route, if sub route is not present, the traffic have to wait till the road is clear for the traffic.

The problems like broadcast storm, building shadow, Intersection are solved by the design used to deploy the network. The Broadcast storm problem is automatically solved because there is no V2V communication and only authenticated vehicles are allowed to send and receive information from the RSUs. Whenever alert message is received by the RSU, it will check for the location id, and time Stamp if the location id is not present with the time stamp, if the information is new RSU will broadcast the message in its respective area to all vehicles and also send an alert message to MA and MA will broadcast that event message to all the RSUs in that area, the broadcast will cover large distance and also increase the efficiency of the broadcast.

The Building Shadow and Intersection is solved because be have RSU on every traffic light, critical areas like bridge, railway crossing etc and every RSU is Fixed distance that is 1000 meter, We know it is bit costly to deploy RSU as we proposed but for the safety of the user it is less considered.

6. SIMULATION RESULT

The following proposed approach is implemented on NS2 using OTCL language.



The simulation result is shown in the diagram; the graph is plotted between x-axis as time and y-axis as efficiency, as the no. of packets in the network increases we can easily depict from graph that delay in packets has not increased while packet loss is also low, with higher throughput.

7. STRENGTH:

By using the number plate of 13 bytes and driving license number of 5 bytes and confidential password of 4 bytes, provides the security against the brute-force attack, because it requires the $2^{22*8}=2^{178}$ numbers of iteration which is significantly large number of iteration.

It adds extra security against social engineering by using confidential password which may randomly chosen by user.

8. CONCLUSION & FUTURE WORK

In this paper the proposed algorithm was used to authenticate a user and uses carry and forward mechanism in order to broadcast data. We have made several assumptions which are quite feasible in real environment. Thus algorithm can perform well in real conditions. We are working on enhancing the algorithm and performance. We are improving some part of algorithm to make it more secure, so that we can provide a safe and secure Environment to users and user can participate in communication without any hesitation. It is only possible if we provide users safe and secure environment, where there is no threat to their security and privacy.

ACKNOWLEDGEMENT

First of all I feel great pleasure in acknowledging my deepest gratitude to my revered guide and mentor, **Mr. Mohinder Kumar**, Professor, Computer Science and Engineering Department, Lovely Professional University, under whose firm guidance, motivation and vigilant supervision I succeeded in completing my work. He infused into me the enthusiasm to work on this topic. His tolerant nature accepted my shortcomings and he synergized his impeccable knowledge with my curiosity to learn into this fruitful result. Words are inadequate to express my heartfelt gratitude to my affectionate parents and my elder brother who have shown so much confidence in me and by whose efforts and blessings I have reached here. I find it hard to express my grateful to the Almighty in words for bestowing upon me his deepest blessings and providing me with the most wonderful opportunity in the form of life of a human being and for the warmth and kindness he has showered upon me by giving me life's best. I wish to express heartiest thanks to my friends Saurabh Srivastava, Sarvesh Kumar, Vijay Kumar, Ramashare Yadav for their support and inspiration.

9. REFERENCES

[1] Shou-Chih Lo · Jhih-SiaoGao · Chih-Cheng Tseng A Water-Wave Broadcast Scheme for Emergency Messages in VANET © Springer Science+Business Media, LLC. 2012

[2] Raya, M., &Hubaux, J.-P. (2007). Securing veehicular ad hoc networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, 15(1), 39–68.

[3] Youngho Park.Chul Sur Kyung-Hyune Rhee. A Privacy preservation Location Assurance protocol for location Aware services in VANET, Wireless communication, spinger

[4] Kanitsorn Suriyapaiboonwattna, ChotipatPornavalai. Goutam Chakraborty. An Adaptive Alert Message Dissemination Protocol for VANET to Improve Road Saftey. FUZZ-IEEE 2009, Korea, Auggust20-24,2009

[5] SaurabhSriavastava, Sarvesh Kumar, Vijay Kumar "all unit interconnection algorithm in VANET", IJCNWMC vol. 3 issue 1 2013

[6] http://www.car-2car.org/index.php?id=46&L=llkptc

[7] http://vnt.disi.unitn.it/usage.php