International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Privacy Preserving and Secret based Navigation Scheme in Vehicular AdhocNetwork : A Case Study

M. Lawanya Shri[*1], M.B.Benjula Anbu Malar[2], G. Priya[3],

K. Santhi[4],M.Deepa[5]

SITE, VIT University, Vellore, Tamilnadu, (India)

ABSTRACT

In this paper, the navigation scheme is provide the actual road condition to compute a better route in an efficient way. The main benefit of this system is that in which it collects the facts from the drivers and provides the appropriate navigation path based on the actual road situation. Drivers can communicate with each other form the RSU (road side unit) and the unit provide the appropriate way based on the drivers queries.it provides the more secrecy and safety for the driver issues through the innominate credential. This strategy is used when the drivers want to avoid the traffic and reach to the destination in the shortest time because it gives the best way for the particular vehicle from the actual road conditions. The main purpose of this strategy is to protect the facts and no one can access the facts. This approach saves the 60% of the travelling time.

Keywords: Navigation, secure vehicular sensor network, verification, pseudo identity, anonymous credential

I.INTRODUCTION

Now a day, they use the GPS in which it will show the map from source to destination path i.e. the shortest way from your origin. Suppose on the particular way there is an accident or traffic jams then you are not able to get this kind of facts in this application [2]. The disadvantage of this application is that you don't know the actual road situations of the particular way. If there is an accident or traffic jam etc. then you can't reach to the destination in the shortest time. By knowing road situations you can easily get the better way from your origin. For this purpose VANET (vehicular ad hoc network) strategy is very helpful to reach to the goal in the shortest time as well as in the without any traffic [3]. VANET is formed by many systems like i.e. used in other domain other purpose.

In this system the one unit is used to transferring the messages from one vehicle to other vehicles this unit is called road side unit it is act like an admin of any system.one vehicle can communicate to another vehicle from this unit in the intimate manner. The issues of the drivers can be solved by the authority and the authority is like a server or any other application. In this system there is a wireless communication between vehicles. There is an only one type of connection i.e. vehicle to framework means only the vehicle can contact with the framework (unit) [3]. This RSU is act like a medium between the vehicles. This system allows conveying the messages to all

the nearby vehicles [11]. It collects the facts from the different drivers and it gives the appropriate navigation way based on the driver's issues. Suppose the driver wants to go from the particular path then driver can ask the way facts from the RSU and then it gives the best, shortest and traffic free way to reach the goal [6]. The transmission of between the vehicles is very intimate no one can retrieve the messages because there is a more safety and secrecy on the messages.

For the safety purpose of the driver's issues the imitated identity and Secure Hashing11 algorithm is used for the sending the messages to the framework for the more safety. For example, any attack is occur the only the authorized party can be retrieve the actual identity of the vehicles based on the imitated identity [10]. The safety and the intimate is more important thing in this type of system because the messages are convey in the intimate manner. By this intimate the messages can't hack by the attacker. There is a free service i.e. provided in this system because from this service anyone can get the appropriate way from this system [5]. There is a more securable service provided. Anyone can register but anyone cannot get the facts. Before giving the facts to the vehicle from the RSU the vehicle must be verified by the imitated identity and then it gives the facts to the particular vehicle [11]. It will automatically search the better way from origin to the goal based on the facts i.e. given by the other vehicles. This strategy has many advantages like it saves the 60% of the travelling time; it gives the shortest way for saving the time etc.

This strategy has many advantages like if suppose you want to reach from origin to goal in the shortest time and also avoiding the traffic on that particular road. This is the best strategy to fulfil these requirements. When you don't know the road situations of the particular road that you want to go then you cannot reach to the destination in the shot time. This approach is very common nowadays, because in old days we use the GPS in this approach only the map show along with the path [2]. But VANET_ gives facts related to that particular way. Suppose on one way there is an accident and there are another ways for the same destination and there is no accident so this fact is shown in this strategy. So by this kind of facts everyone can get the better way from origin to the goal [5]. This is more securable from the other approaches. It shows the actual situation of the particular way. The fact is sends in the encrypted format so by this thing no one can get the facts from the unit. The key is generated for the short period of time because the key must be different at every time [4]. By different key no one can get the facts. The fact is sends along with the key so without any key no one can get the particular facts for the particular vehicle.

The contact between the vehicles can be done easily with the unit. It provides the two way connection from node to node. The vehicle can easily communicate with the vehicle with the keys. These keys are attached with the facts and i.e. generated by the authority. By giving facts to the unit the, the unit can give the better path to another vehicle. By creation of the unique credential is that in which it takes a random number and convert it into the encrypted format by using the SHA algorithm. This algorithm converts the text into the encrypted format and it gives the facts to the unit. Only the authority and the unit know the identity of this particular fact. So by this generation no one can get the particular facts [6]. This approach generates the credential at two different levels first at when the driver gives the facts like speed of the vehicle, location (travel, traffic), type of the traffic etc. and other one is when driver ask for the navigation path to the unit. Two time of the generation is

needed because it gives the efficient safety [8]. The identity must be same at the different levels because it is the same vehicle that is asking for the path.

This strategy has three features first is it verifies the vehicles in efficient way. Second is that the key generation and creation of credential it gives a more safety. Third one is only authority know the credential no one can modify the facts without the keys and credential. This approach gives an advantage to reach the goal in a short period of time.

II.LITERATURE REVIEW

Routing in the network through the access points

The way of the interchanging info in the network must be two ways like one node send the messages to another and then give the messages to back to the node. In this paper, the facts for the particular vehicle can be view like speed of the particular vehicle, traffic facts, road situation, location etc. this messages send in the wireless network. Routing protocol is used to communicate the messages between the vehicles. Through the access points the messages can be only communicated [6]. There is a two way connection like one is the access point to vehicle and the other one is vehicle to access point. Message sends in the packets in the secret manner. In the wireless network the protocol is used to transferring the messages from one host to another host [6]. The vehicles can communicate with only through the points i.e. installed over the network. The one point is connected to another and it sends the messages and replies the messages.

Enhanced verification scheme for sensor networks

Through the sensors you can easily identify the current location of the particular vehicle. Each vehicle has it an own and generated identity through this identity the verification can be easily done [7]. Vehicles can communicate with each vehicle through the framework. This framework is used to convey the messages from on vehicle to other vehicles. From the verification the vehicle you can easily identify the particular vehicle. Through the sensors you can find out the vehicle location now where it is exactly [7]. So by this finding the locations of the particular vehicle you can easily identified and easily get the facts. For safety purpose the verification is performed by the sensors like that is the vehicle on that road. This is the appropriate approach to collect the traffic facts in the dynamically manner. It gives the messages in the form of encryption and then the unit will verify the message and then gives path.

Parking scheme for huge parking area

For finding the vacate area for the parking through the sensors it detects the vehicle location and then it gives the guide signs to the particular vehicles [8]. Where the parking space is available it will show the location to the driver and it is done in an efficient manner. This is very difficult to find the space for park the vehicle so this will help to find the space and then it gives the location where you can park [8]. Suppose there is a very huge traffic on the road and you want to park the vehicle then it is very difficult to find the space. So in this type of situation before you reach the goal you can find out the parking location. To reduce the traffic and collision you

can use this system. This strategy is used nowadays, because it reduces the time for par the vehicle and also reduces the traffic on the particular road.

Innominate credential for secrecy E learning

In this paper, the credential is created along with the specific field like i.e. used in whole system. The main advantages of creation of the credential the safety will be high and the messages are more intimate [10]. It creates the unique identity for the particular vehicle in the network so by this creation of unique identity or imitated identity the secrecy of the navigation strategy must be very high. By reducing the attack this approach is very useful in the network [10]. By using some algorithm it converts the text in some other format then sends the facts to the admin. Every time giving the facts from user to the admin it generates the credentials for the particular facts. Learning system has user and admin for the contact so secure the facts between the user and the admin by using the credentials [10]. It is generated by algorithm and sends to the admin in the different type of format. This is very helpful technique for avoid the attacks.

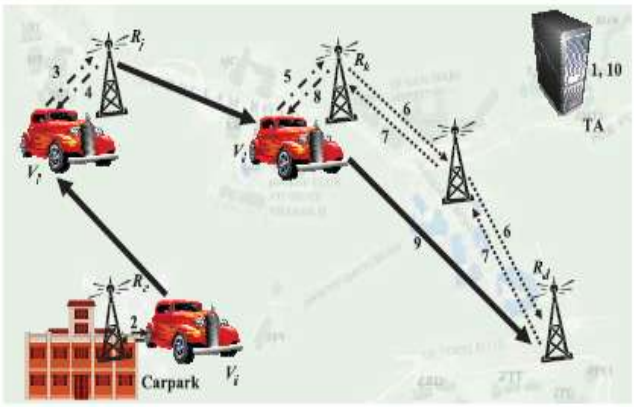
III.PROPOSED SYSTEM AND METHODOLOGY

This system has new idea of providing the navigation ways to the particular drivers. The main advantages of this system are that in which the drivers can easily get the better way from origin to the goal in an efficient manner. The contact between the vehicles to another vehicle is done with the help of the unit which is called RSU (road side unit) [11]. This unit is act like an admin. The drivers can communicate with only with this unit. The trusted authority is act like server or an application i.e. run at the back end of the system. Each vehicle has its own identification for getting the better way from this system.

The authority is generated the credential and the imitated identity for each vehicle for the safety purpose [10]. When the driver gives the facts of the particular vehicle the specific field is encrypted with the Secure Hash1 algorithm like generate credential for the particular vehicle. And when the vehicle sends the request to the RSU for the navigation way from origin to the goal it will again generate the credential for the particular vehicle. Both credential must me matched if it is not matched it means some attack is there [10]. And along with the credential the key also is generated the messages is transferred with the key i.e. the random number for the particular vehicle when the drivers give the facts like traffic location, speed, travel location, weight of the traffic etc. as well as for the path. The generation the key is different at the different location like same vehicle sends any of the facts to the unit then it generates the key for the particular session. This key is only known by the unit. When the request is sent to the unit then it will give the appropriate path to the particular driver [8]. This unit will decrypt the specific field credential and then it sends the messages to the vehicle. It gives the all the facts of the other vehicles i.e. related to the way then vehicle can select the rout whatever the driver wants to go. The unique identity is generated for the two times first at the time when giving the facts to the unit and the one is when the vehicle request for the path from the RSU [11]. This generation must be different at the different levels suppose if this generation is same then anyone can get the facts easily so by this approach to generate the

credential it gives a high safety to this strategy. The SHA1 algorithm is used for encrypt the facts [10]. To improve the performance of the system you must use the algorithms for sending the facts to one to another.

IV.SYSTEM ARCHITECTURE



WORKING

1.) The authority generates the innominate credentials.
2.) The vehicle sends the facts along with the credential and the key to the RSU.
3.) The vehicle request for navigation credential from the RSU and it generates the key again.
4.) RSU verifies both the innominate credentials.
5.) After some distance the vehicle request for navigation path from the RSU.
6.) The navigation request sends to nearby RSU until it reach the destination.
7.) RSU finds the better way for the particular vehicle and verifies the vehicle.
8.) Then it gives the navigation path to the vehicle.

MODULES

- VANET
- Credential generation
- Key generation
- Communication among RSU

VANET

This is first and the important module in which the vehicle can register and enter in the network. It is a network i.e. made up with the sensors, applications, servers, software's, nodes, RSU etc. the connection is done in the in the intimate manner. The authority is like a server to send the messages from one node to another node. Through the sensors the location of the vehicle can be easily detected [1]. Vehicles can communicate with each

other in the network. It is the wireless connected network. The connection is in the two ways one is vehicle to framework and other is framework to vehicle. It is a network the two ways connection is performed like vehicle can communicate with other through the unit. The vehicles are moving around on the road and can share the facts to the other vehicle. The unit collects the facts to the vehicles and share with other vehicles [4]. Through the sensors the location the particular vehicle can be easily detected and finds the vehicle. The fact is shared in the encrypted format because if fact is not encrypted in the network then it must be taken by the attacker [6]. So avoid the attacks in the network us the encrypted text. By using the message passing the facts sends to the other vehicle is easy it is not directly to one driver of the vehicle to other driver of the vehicle [8]. Facts sends to the unit and then unit must be verified by the keys and then it sends the appropriate facts to the appropriate driver of the vehicles. Now use the SHA1 for transmission of the messages in the network.

V.INNOMINATE CREDENTIAL GENERATION

This approach is used for the safety purpose. The safety is most important thing in any type of network. By using SHA1 algorithm generate the text for the specific field to identify and verified the particular vehicle [10]. This is used when sending the facts to the vehicles for knowing the better path. The generation is at the two times when giving the facts to the unit and request to the unit for the particular path. Fact is sends along with the identity and key. This must be different at the different level. The generation of the credential must be same at any of the level through only know the facts of the particular vehicle [10]. The fact of the specific field is to be converted into the different text i.e. only known by the authority or the server [10]. The credential must be same at the different level because if its same then only it is the same vehicle otherwise it is different vehicle is want to access the facts or it is an attacker access the facts. In the network the facts should be in the secret form. Then no one can access the facts.

VI.FRAMEWORK OF SECURE HASHING1 ALGORITHM

1.) Attach protection bits……..

The message must with the protected bits i.e. in the form of 0's and 1's. The length of the message is 64 bits and with this is also diversified of 512.

2.) Attach length……..

64 bits are attached at the last of the message. This messages in the form of binary. These all the bits show the actual message.

3.) Construct the functions……..

It needs 80 functions to be processed.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

4.) Construct the framework……..

It needs 80 function words.

i.

K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)

5.) Compute buffers……..

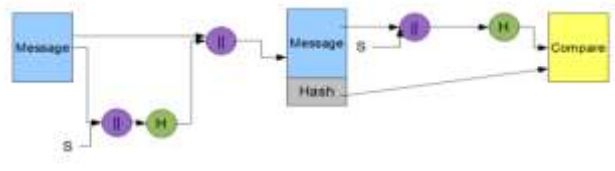
It needs 5 word buffers i.e. to be 32 bits.

H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0

6.) Process the message in 512 bits……..

It generate the loops through attach and protection bits in the 512 bits.

DIAGRAM FOR HASHING FUNCTION

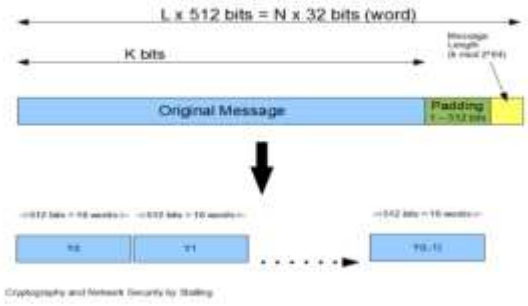


NOTE: No Encryption with sender and destination holding single security key (S).

Cryptography and Network Security by Stalling

DIAGRAM FOR MESSAGE

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354



VII.KEY GENERATION

By the key generation the safety is very high because if suppose you send the messages with key then anyone cannot access the facts because the key will be different at the each and every time. It is a random number generation along with the facts i.e. send by the driver. This fact should be secret in the transmission [1]. By the generation of the identity and the key the secrecy must be very high. The key is verified by the RSU when it replies the path to the vehicles. The key will be the random number from 1 to n-1 and based on the vehicle id it will be generated and then it must be verified [3]. The key is generated at the two different levels one is when giving the facts to the unit and when the request to the RSU for the path. This key must be different at the different levels because if it is not different then it is used by the other person [2]. This keys must be different it is generated for the short period of time thus no one can access the facts. The generation of the particular key is attached with the vehicle. Without this key facts will not to be send to the unit.

VIII.COMMUNICATION AMONG RSU'S

The communication in this unit is on the two ways. It collects the facts of the particular vehicle i.e. moving around the road like location, speed, weight, traffic type etc. after the collecting these kind of facts this unit sends the facts along with path to the drives who request for the path. Collecting and sharing the facts between the vehicles is done with the help of the routing protocol [11]. The fact is sends in the safety manner by the generation of the identity and the generation of the key. The contact between the units is in the two ways.

IX.CONCLUSION

This strategy provides the navigation way to the vehicles in an efficient way. It collects the facts from the driver and sends to the unit in a intimate manner. The safety of the facts is more in this approach. This fulfils the features like the facts is sends with the authenticated manner and it generate the key i.e. attached with the facts etc. it provides the shortest travelling way to the vehicle to reach the destination. The main purpose of this strategy is to protect the facts and no one can access the facts. This approach saves the 60% of the travelling time. It gives the better way based on the drivers facts and these facts properly authenticated by the authority. It

avoids the traffic and collision for the particular way. Is saves the travelling time of the driver. Through the innominate credential and generation of the key must give the safety and secrecy to the vehicle.

REFERENCES

[1] T. Chim, S. Yiu, L.C. Hui, and V.O. Li, "SPECS: Secure and Privacy Enhancing Communications for VANET," Elsevier Ad Hoc Networks, vol. 9, no. 2, pp. 189-203, Mar. 2010.

[2] R. Hwang, Y. Hsiao, and Y. Liu, "Secure Communication Scheme of VANET with Privacy Preserving," Proc. IEEE 17th Int'l Conf. Parallel and Distributed Systems (ICPADS '11), pp. 654-659, Dec. 2011.

[3] D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," IETF RFC3174, 2001.

[4] "Traffic Message Channel (TMC)," http://www.tmcforum.com/,2004. 5. M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security

[5] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services," Proc. IEEE VTS 50th Vehicular Technology Conf. (VTC '99), pp. 2223-2227, Sept. 1999.

[6] G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," Proc. IEEE Fourth Int'l Conf. New Trends in Information Science and Service Science (NISS '10), pp. 393-398, May 2010.

[7] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An Efficient Identitybased Batch Verification Scheme for Vehicular Sensor Networks," in *Proceedings of the IEEE INFOCOM '08*, Apr. 2008

[8] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots," in *Proceedings of theIEEE INFOCOM '09*, Apr. 2009, pp. 1413 – 1421.

[9] D. Chaum, "Security without identification: Transaction systems to make Big Brother obsolete," *Communications of the ACM, Vol. 28*, pp. 1030 – 1044, 1985.

[10] E. Aimeur, H. Hage, and F. S. M. Onana, "Anonymous Credentials for Privacy-Preserving E-learning," in *Proceedings of the IEEE MCETECH'08*, July 2008, pp. 70 – 80.

[11] C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSUAided Message Authentication Scheme in Vehicular Communication Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1451- 1457, May 2008.

[12] B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message Broadcast in VANETs Using Group Signature," Proc. IEEE Fourth Int'l Conf.Wireless Comm. Sensor Networks (WCSN '09), pp. 131-136, Dec. 2008.

[13] Shri, M. L., & Subha, D. S. (2013). An implementation of e-learning system in private cloud. *International Journal of Engineering and Technology*, *5*(3), 3036.

[14] LawanyaShri, M., Subha, S., & Balusamy, B. Energy-Aware Fruitfly Optimisation Algorithm for Load Balancing in Cloud Computing Environments. *Int J IntellEngSyst*, *10*(1), 75-85.

[15] Jothipriya, G., & Shri, M. L. (2013). Database Synchronization of Mobile-build by using Synchronization framework. *International Journal of Engineering and Technology*, *5*(3), 2316-2321.

[16] Malar, M. B. A., Shri, M. L., Deepa, M., &Santhi, K. (2016). Approach for Secure Authorized Deduplication using Hybrid Cloud. *International Journal of Applied Engineering Research*.

[17] Lawanyashri, M., Balusamy, B., & Subha, S. (2017). Energy-aware hybrid fruitfly optimization for load balancing in cloud environments for EHR applications. *Informatics in Medicine Unlocked*.

[18] LawanyaShi, M., Balusamy, B., & Subha, S. (2016). Threshold-Based Workload Control for an Under-Utilized Virtual Machine in Cloud Computing. *International Journal of Intelligent Engineering and Systems*, *9*(4), 234-241.

[19] M. B. BenjulaAnbu Malar, M. Lawanya Shri, M. Deepa3, K. Santhi "Approach for Secure Authorized Deduplication using Hybrid Cloud ",INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH,2016.

[20] K.santhi, M.deepa, M.Lawanyashri, M. B. Benjulaanbu malar "an efficient active audit services for achieving data integrity in cloud system", international journal of pharmacy & technology,2016.

[21] S. pavithra , M. lawanyashri, "privacy preserving the electronic health record using encryption protocol in cloud computing", international journal of pharmacy & technology,2016.

[22] M. Lawanya Shri, M.B.BenjulaAnbumalar, K. Santhi, Deepa.M ,, E-Learning System With Hierarchical Attribute Set Based Encryption Access Control In Cloud" ", International Journal Of Pharmacy & Technology,2016