Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 7, July-2017

Group Based Authentication in V2V Network Using Decentralized Light Weight Protocol

Snehal M. Choudhari[1], Hirendra R. Hajare[2]

[1]*M. Tech Scholar, Dept of Computer Science and Engineering, Ballarpur Institute of Technology, Ballarpur, Maharashtra, India*

[2]*HOD, Dept of Computer Science and Engineering, Ballarpur Institute of Technology, Ballarpur, Maharashtra, India*

Abstract — Vehicular ad hoc networks (VANETs) are an important communication paradigm in modern-day mobile computing for exchanging live messages regarding traffic congestion, weather conditions, road conditions, and targeted location-based advertisements to improve the driving comfort. In such environments security and intelligent decision making are two important challenges needed to be addressed. In this paper, a trusted authority (TA) is designed to provide a variety of online premium services to customers through VANETs. Therefore, it is important to maintain the confidentiality and authentication of messages exchanged between the TA and the VANET nodes. Hence, we address the security problem by focusing on the scenario where the TA classifies the users into primary, secondary, and unauthorized users. In this paper, first, we present a dual authentication scheme to provide a high level of security in the vehicle side to effectively prevent the unauthorized vehicles entering into the VANET. Second, we propose a dual group key management scheme to efficiently distribute a group key to a group of users and to update such group keys during the users' join and leave operations. The major advantage of the proposed dual key management is that adding/revoking users in the VANET group can be performed in a computationally efficient manner by updating a small amount of information. The results of the proposed dual authentication and key management scheme are computationally efficient compared with all other existing schemes discussed in literature, and the results are promising.

Keywords- VANET, V2V Communication, RSU, Communication, PKI, Authentication, TA

I. INTRODUCTION

The vehicular ad hoc network (VANET) is a kind of wireless ad hoc network which deploys the concept of continuous varying vehicular motion. Here, the moving vehicles act as nodes. It is an active area research right now and emerging type of network aimed at improving safe driving, traffic optimization, and some other services through the vehicle to infrastructure communication (V2I) or vehicle to vehicle communication (V2V). It plays an important part in intelligent transportation system (ITS). Each vehicle communicate send and receive messages by On Board Unit (OBU) and equipped with Event Data Recorder, GPS, Trusted component etc. The Roadside Units (RSU) is responsible for broadcasting safety messages periodically. With recent advances in the development of Wireless communications protocols and plummeting costs of hardware needed, along with the automobile industry's desire to increase road safety and gain competitive edge in the market, Vehicles are equipped with latest communication hardware, GPS etc. hence becoming Computers on Wheels or computers networks on wheels. But wireless communication is itself susceptible to various attacks, hence the security of VANET cannot be undermined. Some malicious vehicle may send false information into the network to gain an unfair advantage on the road or to cause serious accidents. Hence the sender vehicles should be authenticated by the receiver before taking any action based on the received safety message. Normally origin authentication is provided by digital signature with the help of certification services. In VANET, a Trusted Authority (TA) serves the purpose, but it involves huge communication overhead and also a vehicle have to communicate with TA via RSUs. Now RSUs are fixed infrastructures along the road, which periodically broadcast safety related information, Typically RSUs placed over every 300m to 1 km and they broadcast at the interval of every 300ms. Hence placing RSUs along a long highway to provide omnipresent infrastructure is not feasible economically for now. Hence vehicle should be able to authenticate others with limited help from TA or fixed infrastructure. Also in VPKI, the public keys are bound to the identity of the vehicles in certificates, hence an eavesdropper may track the sending vehicle, but we need to protect the privacy as well.

Hence in our research, we propose an OBU based authentication scheme for V2V communication, where the vehicles generate self-certified public/private key pairs with the help of a check value computed by TA and initially given to Vehicles during registration. The Check value is computed via one way hash chaining mechanism. The same check value is given to multiple vehicles in order to achieve privacy. But a tracking hint is attached to all the sent messages by default, which can later be used to identify a vehicle. Also, group formation is done so that all the vehicles send their messages to Group leader, then the Group leader sends the aggregated message to all for reducing communication overhead. Our research is solely focused on authentication of vehicles, hence it is possible that an legitimate vehicle of

All Rights Reserved, @IJAREST-2017

the network i.e. authenticated vehicle may send false information with malicious intent. Hence, in that case, the reliability of messages comes into the scene, which is beyond the scope of our research. But we assume that vehicle does evaluate the reliability of messages using existing optimal schemes, which can later be used for revocation purpose.

II. DATA COMPRESSION ALGORITHM

2.1 LZW Compression Algorithm

LZW compression algorithm is a dictionary based algorithm which always outputs a code for a character. Each character has a code and index number in the dictionary. Input data which we want to compress is read from the file. Initially, data is entered in the buffer for searching in the dictionary to generate its code. If there is no matching character found in the dictionary. Then it will be entered as anew character in the dictionary and assign a code. If the character is in the dictionary then its code will be generated. Output codes have less number of bits than input data. This technique is useful for both graphics images and digitized voice.

Compression example: consider a string "BAABAABB" is given to LZW algorithm. Figure 2 shows the steps done by LZW to generate the output code is "1211211C". In the following example when input string (BAABAABBC) is given as a text to LZW compression algorithm. Initially, every single character will save in buffer. When 'B' is moved to buffer "parse string" then it will replace by 1. The character has its own ASCII code of 7 bit. In the case of B, it has 65 as ASCII code. But in the dictionary, it will replace by 1. So, less number of bits will be used to represent a character. Similarly, AA will move forward and generate its code which is also fewer bits than original. BAA is saved in buffer its code is generated from both AA and B's codeword that is defined as 12. At last when the full string has been searched in the dictionary then its output will be generated as 1211211C.

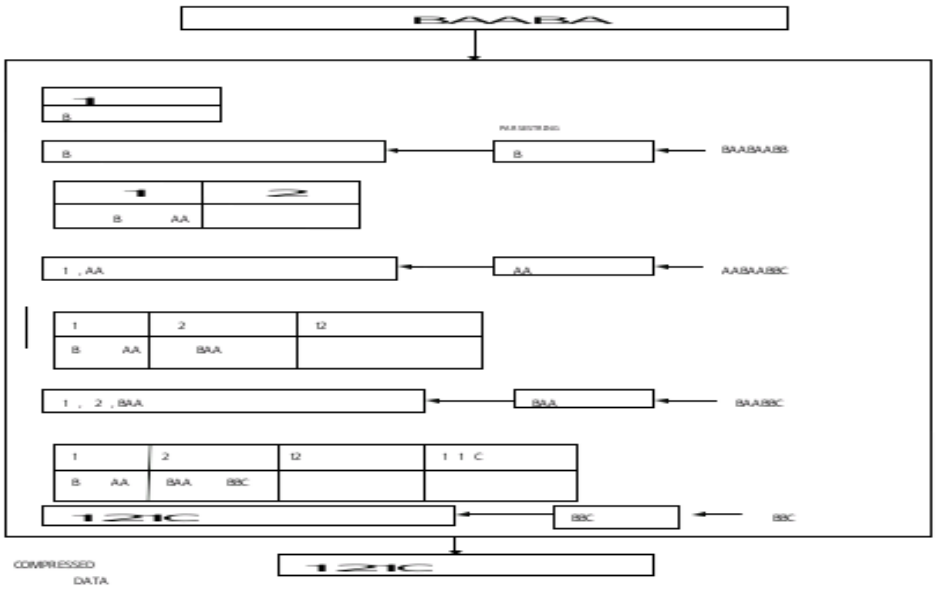


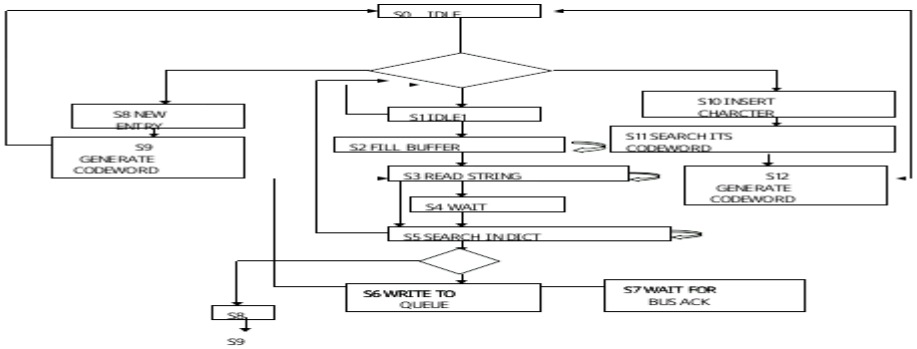
Figure 1: Example of LZW algorithm

2.2 LZW Decompression Algorithm

In LZW decompression algorithm, it needs to take the stream of code output from the compression algorithm and use them to exactly recreate the input stream. Decompression algorithm is shown as:

2.2.1 IMPLEMENTATION OF LZW ALGORITHM

The proposed finite state machine diagram of LZW algorithm is shown in figure 2.



All Rights Reserved, @IJAREST-2017

Figure 2: Finite state machine Diagram of LZW algorithm

LZW algorithm initially has an idle state. A new character has been added to the dictionary when no longer match will found in the search process. LZW algorithm is executed state S8 for performing adding operation in the dictionary. Dictionary is based on content access memory technique which has both contents as well as code in it. Content access memory is a special type of memory used for fast accessing data from memory. In the proposed system, initialization of compression signal is done before to perform LZW algorithm. Input data is entered to LZW algorithm through the file. The proposed algorithm shifted whole input data to buffer which is defined in theS3 state. Every single character has been searched in content access memory. If match signal is '1' then the character was found in the dictionary. Then thecode is transmitted to output buffer "de11". LZW decompressor must construct same steps like a compressor. Decompressor has reviewed thesame process since it is possible to have input codes for searching in dictionaries to recreate its original string. Individual character's code can be also viewed in the dictionary.

III. PROPOSED WORK

We are going to describe the proposed system and its implementation. n the proposed work, we are using the LZW compression algorithm which will compress the requests sent by the new and existing nodes to the group heads. This will reduce the network load and thereby increase the speed of authentication by the system. Also, this will add another layer of security to the system by converting the data from original format to a compressed and secure format

In the system, we are using the following procedure for node authentication,

1. Suppose Node N1 wants to communicate with Node N2 (N1 Source, N2 Destination)

2. N1 first finds a nearest authorized node by using the nearest neighbor technique, suppose this node is Node BS (call it as base station)

3. N1 sends data to BS, and BS sends an ACK to N1

4. N1 sends it's key to BS, and BS checks if key is registered for N1 or not

5. If key is registered, BS asks N1 to send its data, BS checks this data and sends it to N2

6. If key is not-registered, all communications from N1 are blocked

7. We are applying LZW compression technique while sending data from N1 to BS and then from BS to N2.

The figure below shows the procedure of the proposed system.

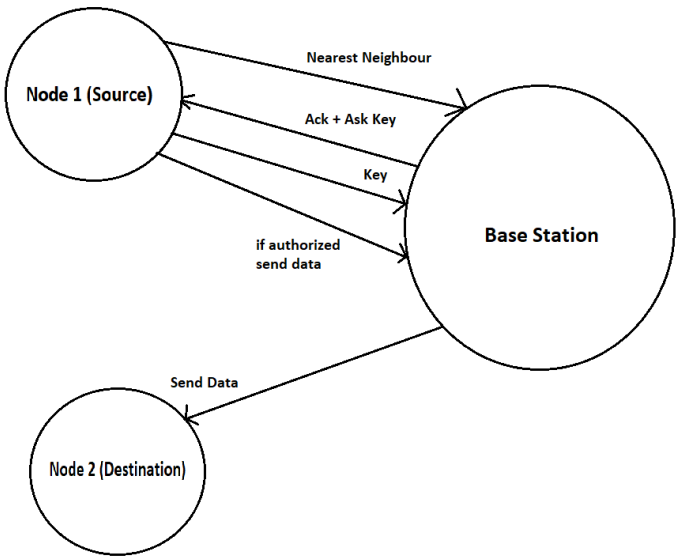


Figure 1: Proposed system Procedure

The system is divided into multiple Modules; the modules are explained as follows:

1. Network formation with communication between vehicles

All Rights Reserved, @IJAREST-2017

2. Development of group based authentication

3. Speed evaluation for the group based authentication protocol

4. Development of LZW algorithm for improving algorithm speed

5. Evaluation of the new protocol and comparison.

A. Network Formation with Communication Between Vehicles

In this module, the network is created between various vehicles and their connection is setup. When the system is mobile and moves between various stations the node is reattached to the base station of the zone. This part of the system is designed in NS2 using Linux as its base.

B. Development of Group Based Authentication

The second module is the development of the authentication. There are seven steps. Suppose Node N1 wants to communicate with Node N2 (N1 Source, N2 Destination). N1 first finds a nearest authorized node by using the nearest neighbor technique, suppose this node is Node BS (call it as a base station). N1 sends data to BS, and BS sends an ACK to N1. N1 sends its key to BS, and BS checks if the key is registered for N1 or not. If the key is registered, BS asks N1 to send its data, BS checks this data and sends it to N2. If the key is not-registered, all communications from N1 are blocked. We are applying LZW compression technique while sending data from N1 to BS and then from BS to N2.

C. Speed Evaluation for the Group Based Authentication Protocol

Since there are a lot of steps speed evaluation is important for the proposed technique. The system takes multiple instructions at the same time, for example, the system sends the Acknowledgement and receives the key at the same time. The delay is also reduced with the help of faster processing.

D. Development of LZW Algorithm for Improving Algorithm Speed

In this module, the development of LZW algorithm is done. LZW starts out with a dictionary of 256 characters (in the case of 8 bits) and uses those as the "standard" character set. It then reads data 8 bits at a time (e.g.,'t', 'r', etc.) and encodes the data as the number that represents its index in the dictionary. Every time it comes across a new substring (say, "tr"), it adds it to the dictionary; every time it comes across a substring it has already seen, it just reads in a new character and concatenates it with the current string to get a new substring. The next time LZW revisits a substring, it will be encoded using a single number. Usually, a maximum number of entries (say, 4096) is defined in the dictionary so that the process doesn't run away with a memory. Thus, the codes which are taking place of the substrings in this example are 12 bits long (2^12 = 4096). It is necessary for the codes to be longer in bits than the characters (12 vs. 8 bits), but since many frequently occurring substrings will be replaced by a single code, in the long haul, compression is achieved.

E. Evaluation of the New Protocol and Comparison.

The system is evaluated on the following parameters:

a. Delay: The total time required by the processes of sending and receiving the data comes under delay parameters. The delay is calculated by adding the time required for various operations such as the request, finding the optimal path, sending data and receiving data.
b. Jitter: It is termed as the network consistency, which helps in finding the network strength and consistency at all levels. Which is calculated by the current delay – Average delay. The best jitter is when the values calculate is 0.
c. Packet Delivery Ratio (PDR): It is the ratio of a number of packets sent by the transmitter to the number of packets actually being delivered. The best PDR is when the PDR is 1 i.e. all the packets reached its destination.
d. Energy: it is the total energy required by the system to perform a single transaction. The energy is inversely proportional to efficiency the less the energy is used the more efficient is the designed system.
e. Throughput: It is the rate of its reaching the destination per unit time. It shows the efficiency of the nodes to process received data.
f. Routing Load: It illustrates the number of calculations required by the network to transfer the data. The lower the load the more efficient is the network.

All Rights Reserved, @IJAREST-2017

IV. SIMULATION RESULTS

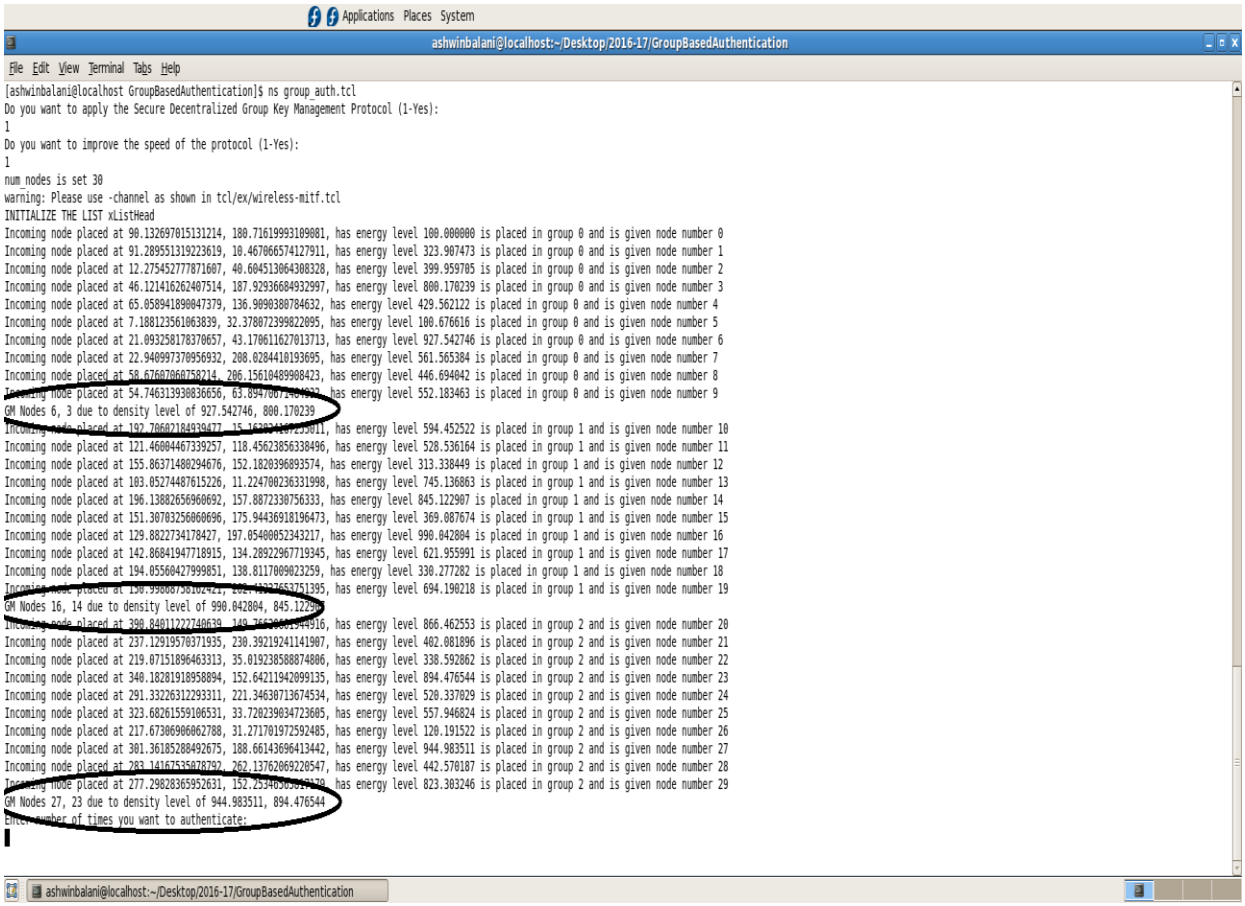


Figure 3: Group and Nodes

The above figure illustrates the Group Manager and nodes. It shows the node number and its density level.

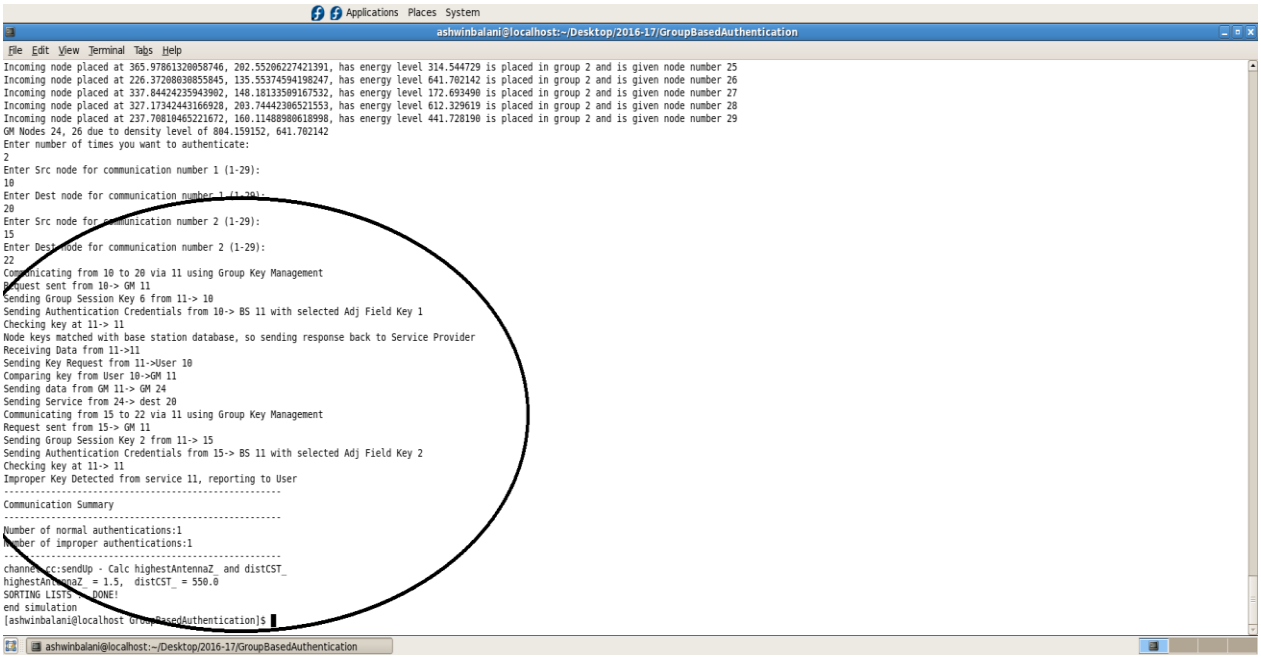


Figure 4: New Authentication

All Rights Reserved, @IJAREST-2017

The above figure illustrates the new authentication in the NS2 for the source and destination node.

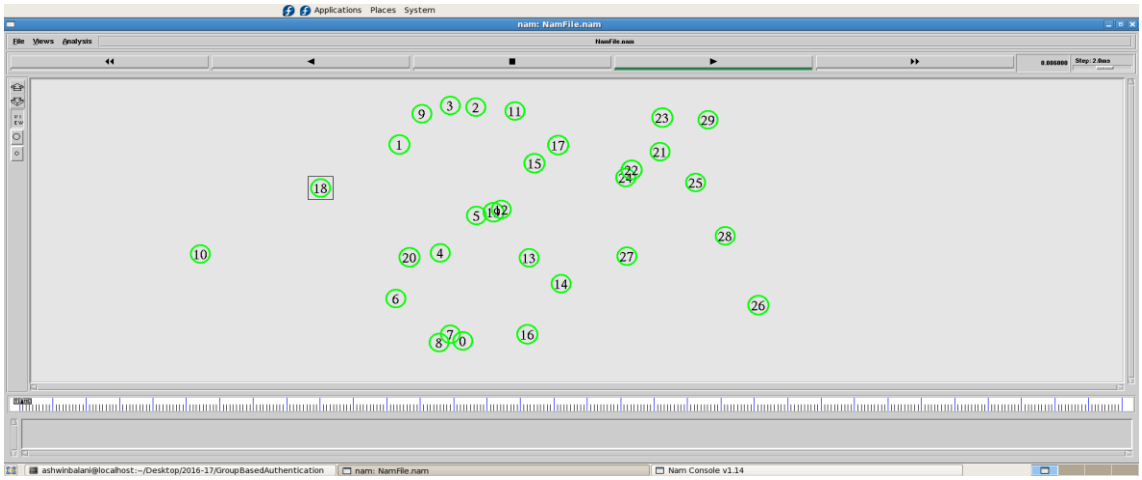


Figure 5: Communication Setup

Here the number shows the number of nodes, the square block shows the base station.

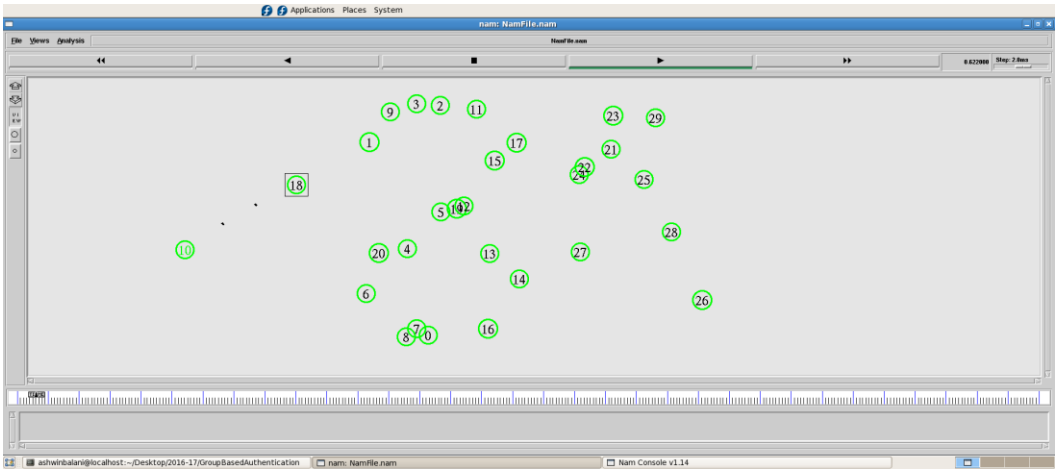


Figure 6: Communication between source and base station

The above figure illustrates the communication between the source and the base station.

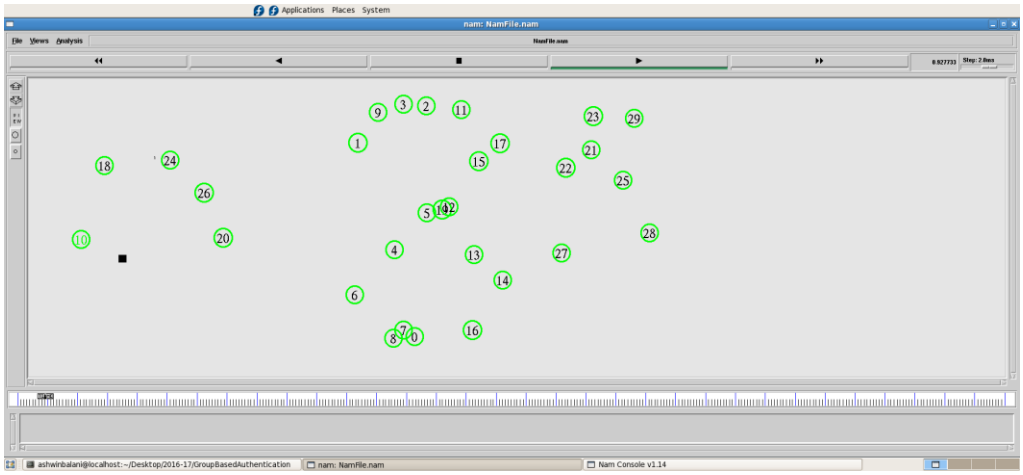


Figure 7: Figure LZW communication

The base station sends an ack and receives the data and finds the destination.

All Rights Reserved, @IJAREST-2017

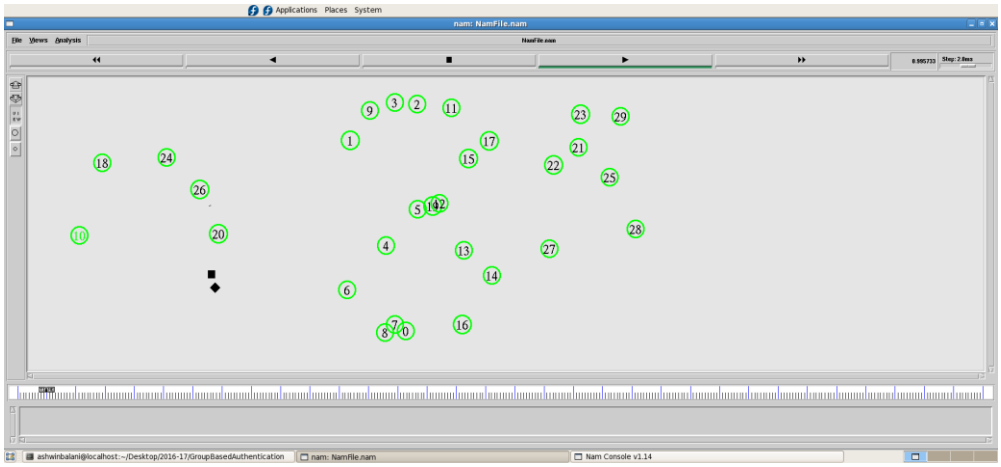


Figure 8: sending data to the destination.

The figure above illustrates the processing and sending of the data to the destination node.

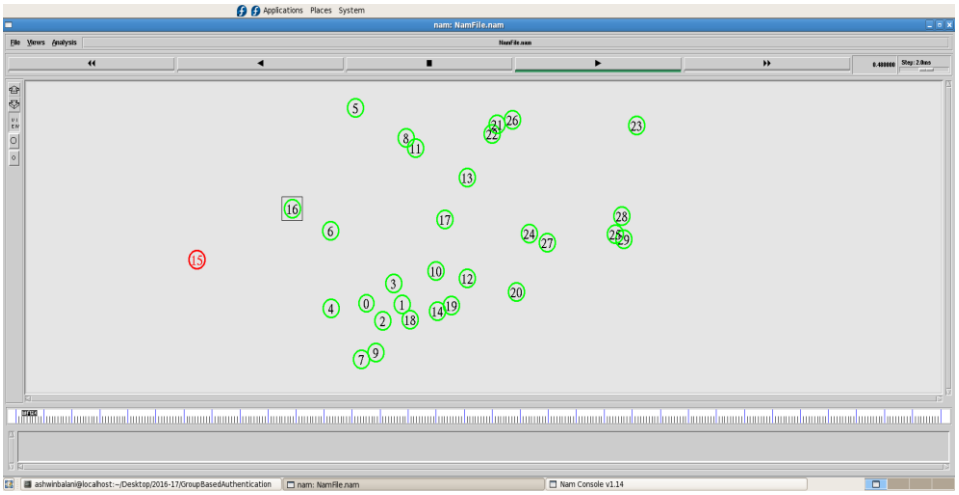


Figure 9: Improper Communication

When the keys don't match the system makes that node as improper (Red color node) as shown in the above figure.

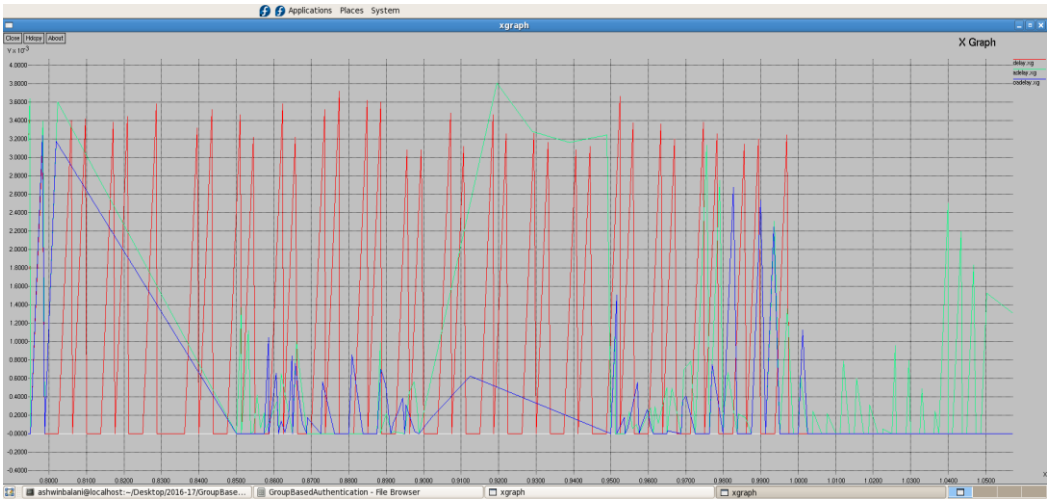


Figure 10: Delay Evaluation

All Rights Reserved, @IJAREST-2017

The system optimizes the delays the blue line in the graph illustrates the proposed technique's delays. The delay is lower than the normal and authenticated technique.

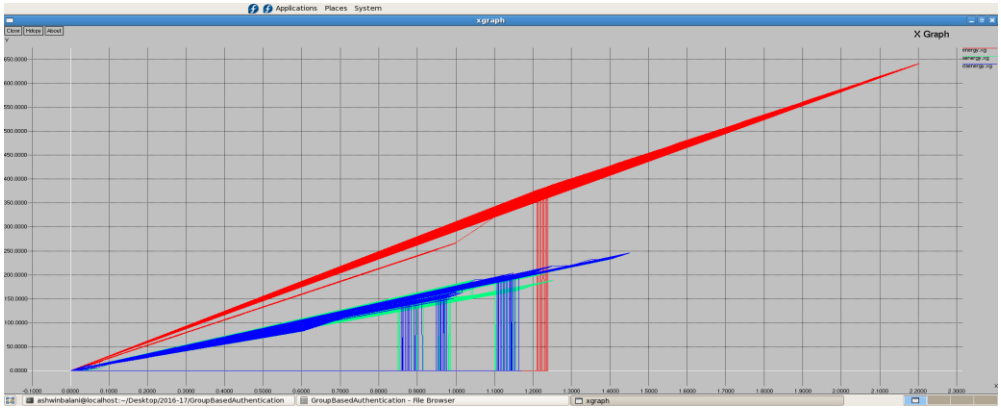


Figure 11: Energy Evaluation

The energy required by the technique is much less than the normal method. As observed from the above graph it shows that the system requires very less energy than the standard technique.

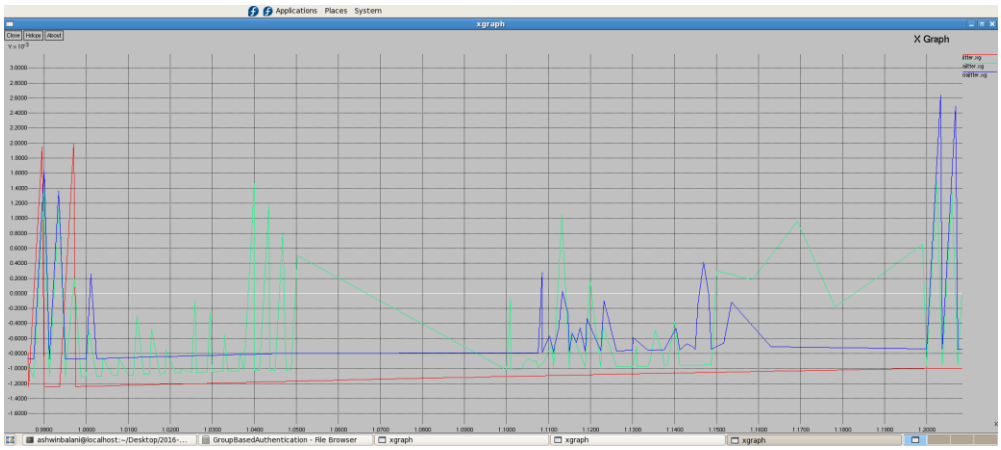


Figure 12: Jitter Evaluation

The above figure illustrates the jitter and it shows that the optimized techniques have the best jitter.

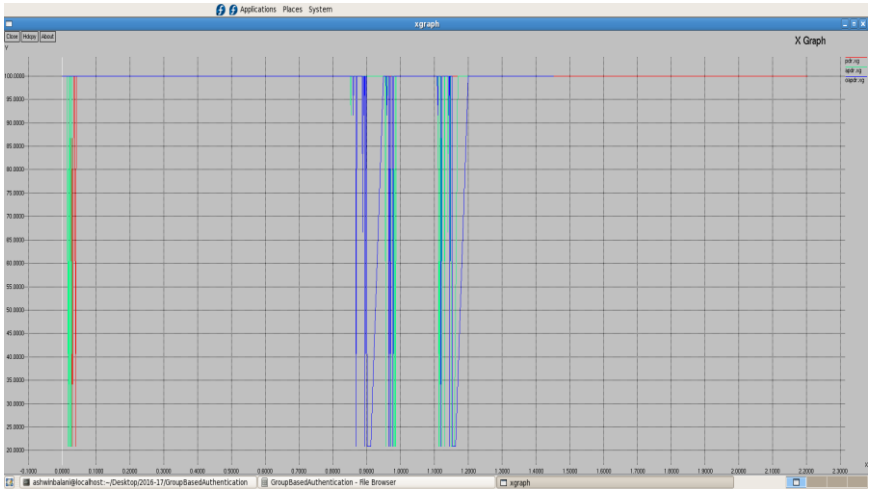


Figure 13: PDR Evaluation.

The above figure illustrates the PDR and it shows that the optimized techniques have the best PDR.

All Rights Reserved, @IJAREST-2017

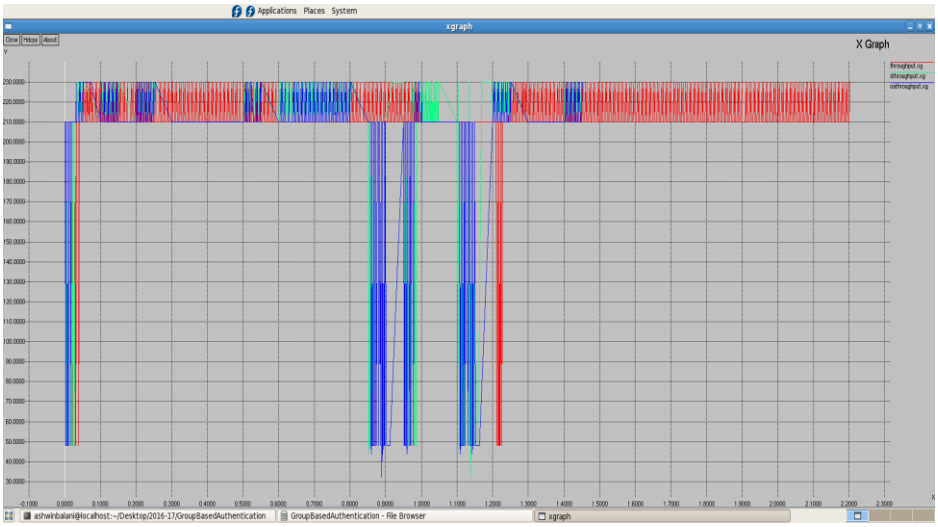


Figure 14: Throughput Evaluation

The above figure illustrates the throughput and it shows that the optimized techniques have the best throughput.

V. CONCLUSION & FUTURE SCOPE

In our work, we proposed an On Board Unit Based Authentication for V2V Communication in VANET which can operate effectively with limited support of fixed infrastructure when there is a lack of it. Our proposed Scheme also forms groups between vehicle-based on their mobility pattern to share traffic related information. The group leader receives and authenticates the messages from the vehicles and then sends the aggregated information to the network which reduces network overheads. By this scheme, the privacy of vehicles is also protected. But most importantly, it drastically reduces the overhead on TA as neither the TA have to store all the key pairs for revocation purpose nor the TA have to authenticate each vehicle. Also, less dependency on fixed infrastructure results in reduced cost, as the infrastructure needed for VANET will take a lot of time in coming days to be fully implemented, till then our scheme can be an effective way to authentic vehicles.

Although our work only deals with Authentication of the message, there is considerable concern regarding there liability of messages and subsequent evaluation for revocation. So this work can be further extended for checking there liability of messages as well as the design of parameters for an efficient certificate revocation procedure.

REFERENCES

[1] Al Sakib Khan Pathan: A book: where a chapter is A Security in VANET- YEet to yet be published.

[2] Fay Hui: A survey on the characterization of Vehicular Ad Hoc Networks routing solutions.

[3] AntoniosStamoulis(antonios.stampoulis@yale.edu),Zheng Chai: A Survey of Security in Vehicular Networks.

[4] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, Xuemin (Sherman) Shen: AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks.

[5] Zheng: Challenges in vehicular networks.

[6] Maen M. Artimy, William Robertson, and William J. Phillips: CONNECTIVITY IN INTER-VEHICLE AD HOC NETWORKS.

[7] Jijun Yin Tamer ElBatt Gavin Yeung Bo Ryu: Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks.

[8] S.Y. Wang: Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways.

[9] Linda Briesemeister Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks.

[10] Yong Hao, Yu Cheng, and Kui Ren Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs.

[11] Wenmao Liu, Hongli Zhang and Weizhe Zhang An autonomous road side infrastructure based system in secure VANETs.

[12] UneThoingRosi and Chowdhury Sayeed Hyder A Novel Approach for Infrastructure Deployment for VANET.

[13] Raya, Maxim, and Jean-Pierre Hubaux. ”Securing vehicular ad hoc networks.”Journal of Computer Security15.1 (2007): 39-68.

All Rights Reserved, @IJAREST-2017

[14] Calandriello, Giorgio, PanosPapadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. ”Efficient and robust pseudonymous authentication in VANET.” InProceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19-28. ACM, 2007.

[15] Lin, Xiaodong, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. ”GSIS: a secure and privacy-preserving protocol for vehicular communications.”Vehicular Technology, IEEE Transactions on56, no. 6 (2007): 3442-3456.

[16] Chaum, David, and Eugene Van Heyst. ”Group signatures.” InAdvances in Cryptology EUROCRYPT 91, pp. 257-265. Springer Berlin Heidelberg, 1991.

[17] Verma, Mayank, and Dijiang Huang. ”SeGCom: secure group communication in VANETs.” InConsumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, pp. 1-5. IEEE, 2009.

[18] Lu, Rongxing, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. ”ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications.” InINFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.

All Rights Reserved, @IJAREST-2017