HMAC Based Secure Authentication of VANET's

Swagat. S. Gudagudi[1], Dr. Veena Desai[2]

[1]Post Graduation Department, Dept. of ECE, KLS GIT, Belgaum, India

[2]Prof Dept. of ECE, KLS GIT, Belgaum, India

Abstract: ***The Vehicular Ad-hoc Network (VANET) has been studied in many fields since it has the ability to provide a variety of services, such as detecting oncoming collisions and providing warning signals to alert the driver. The services provided by VANET are often based on collaboration among vehicles that are equipped with relatively simple motion sensors and GPS units. Awareness of its precise location is vital to every vehicle in VANET so that it can provide accurate data to its peers. Hence the data in VANET communicating between sender and receiver must not be revealed or modified by other impersonators or other vehicles participating in network. In this proposed work the authentication of the vehicles(nodes) by using Hash based message authentication of nodes is computed and the message digest function can be used of either MD-1, 256,512 for the message integrity and the symmetric key mechanism is performed. The simulation is done by using MatLab tool.***

Keywords: component; Authentication, Privacy, Private, VANET

1. Introduction

Wireless adhoc network has become one of the prime topics of research in the very recent years where majority of the research work is concentrated on restricted user-groups, where various nodes cooperate to communicate [1]. A Vehicular Ad-Hoc Network or VANET is a form of Mobile Ad-Hoc Network or MANET which provides communication between vehicles and between vehicles and road-side base stations. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET is different from MANET due to high mobility of nodes and the large scale of networks. Security and privacy are the two main concerns in designing a VANET. Although there are many proposed solutions for improving securities in VANET but security still remains an unsolved research subject. The privacy preserving of data or credential is essential in VANET, which is done by complex cryptographic actions [2]. Many researchers are working on privacy preserving of data in VANET with new type of techniques [3]. Hence there is necessity of protection of any confidential data while communicated through other nodes or vehicles in VANET. As technology is evolving nowadays the payment systems and transmitting of data is through digitized form [2]. Since VANET is a distributed network and dynamic in nature [3], the credential of driver like the license of vehicle, scanned image of passport, any images captured while travelling which is of confidential nature has to be sent to the desired destination. However in order to send this data a suitable privacy preserving of data using some cryptographic actions with less computation time is of highly essential.

The phenomenon of privacy preserving guarantees that the vehicle is anonymous and untraceable as well as it also safeguard the driver's private information during sharing of information with other nodes or vehicles existing in the network [4]. However any attacker can misuse privacy preserving mechanism to provide false information to other vehicles and attempt to reveal any of confidential data that will be transmitting in network. Hence there is a critical need of an effective and robust security mechanism for protecting the confidential data.

In proposed work, we illustrate a novel and yet simple technique for preservation of any credential or the data that is to be sent from source to destination in form of vehicle-to-vehicle communication in VANET. We consider the data input as two images where the first image will be registered license plate image and second image will be the confidential data that needs to be sent via secure channel in a vehicular network. We also use the symmetric key mechanism by using secret private key that will be only known by sender and receiver. Finally, we utilize an embedding technique to send the data with encryption of real data such that it takes less computation for processing.

In the proposed paper, a privacy preservation of data in VANET by using images is discussed. In section 2, we give an overview of related work which identifies all the major research work being done in this area. Section 3 highlights about the proposed system describing the architecture of work and assumptions. Implementation of Proposed system is discussed in Section 3 followed by results and discussions in Section 4 and finally in section 5 we make some concluding remarks.

2. Related Work

This section discusses about the previous research works conducted that were used for preserving privacy of data and the suitable techniques that are used for maintaining the privacy of data. The below are some of the significant research works that are done for privacy preserving of data.

The concept of secret key mechanism for credential has been explained thoroughly by Chaum [2]. In his work, the author explains about the electronic payment systems and the evolvement of paper documents to digital data. The noted author also explains about the pseudonyms and the secret key maintenance for privacy preserving of data along with the private key mechanisms for maintaining confidentiality. The author demonstrates the basic credential and transactions systems with suitable examples. The author has also elaborated the consumer transactions with respect to communication, payment, and credential.

In [5], authors have discusses about various privacy considerations for E-learning *i.e.* anonymous credentials for E-learning systems (ACES). The work demonstrated that in order to achieve full privacy of data for maintaining the communicating data to be confidential requires more challenging and thereby more sophisticated cryptographic tools for computation are required. They also explain that for E-learning activities for unknown courses of privacy preserving achieved by performing computation with encrypted functions.

In [6], authors have discussed about the security issues in vehicular adhoc network (VANET). The authors demonstrated that robust VANET strongly depends on efficient security and privacy features. The work has also discussed about the attack and threats that occurs in VANET system and their mitigation technique towards attack.

The authors quoted that for preserving the real identity of driver the electronic license plate was used. They also discusses the usage of Public Key Infrastructure (PKI), using Digital Signatures (DS), distributing Certificate Revocation Lists (CRL) among vehicles or nodes etc.

In [7], authors have proposed a scheme named AMOEBA that provides location privacy by mitigating the location tracking of vehicles, and protects user privacy by providing vehicles with anonymous access to location based service (LBS) applications. The authors have addressed location tracking by a restricted passive adversary and showed the positive feasibility to successfully alleviate the location tracking by utilizing the separation between road side units and the transmission power control capability of vehicles.

In [8], authors have proposed a scheme called RSU-aided message authentication called RAISE. The accomplished results were found with lowest message loss ratio and communication overhead than both the PKI-based and the group signature based schemes without losing the desired security and privacy requirements in VANETs. The scheme was found much more advantageous than all the prior conventional works because of its less computation and communication overhead. RAISE also protects the privacy of vehicles by adopting the k-anonymity approach.

In [8], authors have proposed a new protocol for preserving privacy for users in VANET that is based on probabilistic key distribution and a security threshold scheme. This scheme provides an efficient and scalable group communications, and at the same time preserves the privacy of the users.

The standard security parameters in vehicular communication system (e.g. integrity, confidentiality, anonymity, traceability and non-repudiation) are important factors to be considered such that in [4] the authors have proposed a secure communication and privacy preserving scheme of VANET. The authors have proposed a scheme that was an efficient self-generated pseudonym mechanism based on Identity-Based Encryption (IBE) to provide privacy preservation.

Reviewing the preliminary research studies above, it can be concluded that privacy preservation of data in VANET is one of the potential factors to be considered for safeguarding the security standards in VANET. The prime focus of the study is to design privacy preservation of data in VANET by using images such that the data and the confidential credential is embedded into it by using secret or private key. The credential is encrypted and embedded with vehicle license plate which gives extra security for preserving of data in VANET.

3. Proposed System

Implementation of proposed security framework application is always preceded by important decisions regarding selection of the platform, the language used, etc. these decisions are often influenced by several factors such as real environment in which the system works, the speed that is required, the security concerns, and other implementation specific details. Basically the proposed framework is implemented in MatLab a technical computing tool. The algorithms and MatLab codes that we have used for implementation are described in detail in next sections. The proposed frame work is modeled using the hash based message authentication, where the two functions or the data is used The system architecture can be shown in figure 3.1. The explanation of it is as follows,

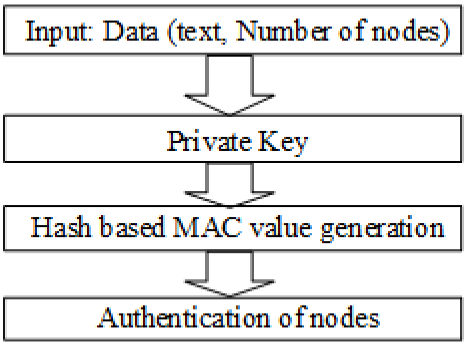

Input: Data (text, Number of nodes)
Private Key
Hash based MAC value generation
Authentication of nodes

Figure 3.1: Proposed System Architecture

- **Input Data:** The data in the proposed work is the text data.
- **Private Key:** The private key is the secret key which will be known by only the source node and the destination node.
- **Hash based MAC value generation:** HMAC is used for mutual authentication of nodes. It can use either Message Digest (MD)-1, or of 256 bits,512 bits for hash generation.
- **Authentication of Nodes:** The authenticated nodes can be seen at output of graphic user interface.

The proposed system uses the concept of HMAC to build a security tunnel among two nodes in VANETs. It is as follows, initially using the concept of RSA a token is generated which is pre- distributed among the two nodes which are in need of communication by the Trusted Third Party (TTP). And once the token is distributed among the source and destination node, the role of TTP ends. TTP

doesn't involve in further communication. On receiving the token from TTP the source node uses the token to calculate session key. And using that session key of source node HMAC is calculated at the source node. And destination node also follows the same procedure and calculates its own HMAC. Now a authentication request message is sent to destination node to source node which consists of the token given by TTP. On receiving the request from source node destination node verifies received token with its token. If both the token's match destination node replies to source node with a reply message which consists of HMAC of destination node. Source node verifies both HMAC's on receiving the reply message from destination node and if both HMAC's match replies to destination node by an acknowledgement message.
The detailed steps for proposed protocol:

Consider a TTP and communication is between node A and node B. And notations used in protocol.

Q	A large prime number.
AReq	Authentication Request Packet
BRes	Authentication Response Packet
P	Point on elliptic curve
A	Long term secret of node A
B	Long term secret of node B
SKAB	Session key generated between node A and B
SKBA	Session key generated between node B and A

Step 1: TTP calculates the token and distributes it among node A and node B.
Step 2: On receiving token from TTP. Node A selects rA randomly, where 1 ≤rA ≤ q − 1 and then computes QA = rA .P. And node A sends Authenticated request packet AReq (tokenA, QA).
Step 3: After receiving AReq message, node B first verifies node A's token. If the A's token is verified using the B's token given by TTP.
Step 4: Node B selects randomly an integer rB in the range 1 ≤ rB ≤ q−1 and computes QB = rB ·P . It then computes SKBA = H ((rB+b) · (QA+PubA)) as a session secret key between A and B.
Step 5: Node B computes HMACB = H(SKBA ||H((QA.x + QB.x)||(QA.y + QB.y)). It then constructs a message m consists of HMACB and QB, that is, m = HMACB||QB and generates a signature sigB (m) on m as sigB (m) = (r,s) using the private long-term key b of B with the help of ECDSA signature generation algorithm. Node B finally sends BRes(m, sign (m)) as an authentication reply message to node A.
Step 6: After receiving BRes message, node A first verifies the signature sigB (m) using the public key of node B with the help of ECDSA signature verification algorithm. Node A then computes SKAB = H ((rA+A) · (QB+PubB)) as a session secret key between A and B. And then calculates HMACA = H (SKAB ||H ((QB.x + QA.x)||(QA.y + QB.y))
Step 7: Node A compares both HMACA and HMACB for integrity check and if the check holds then as an initiator node A sends an authentication acknowledgement message to node B. In this way both node A and node B use the secret key future communication.

The following pseudo code shows the implementation of the proposed system. Enter the number of nodes and source node and destination node.

A. Authentication request message

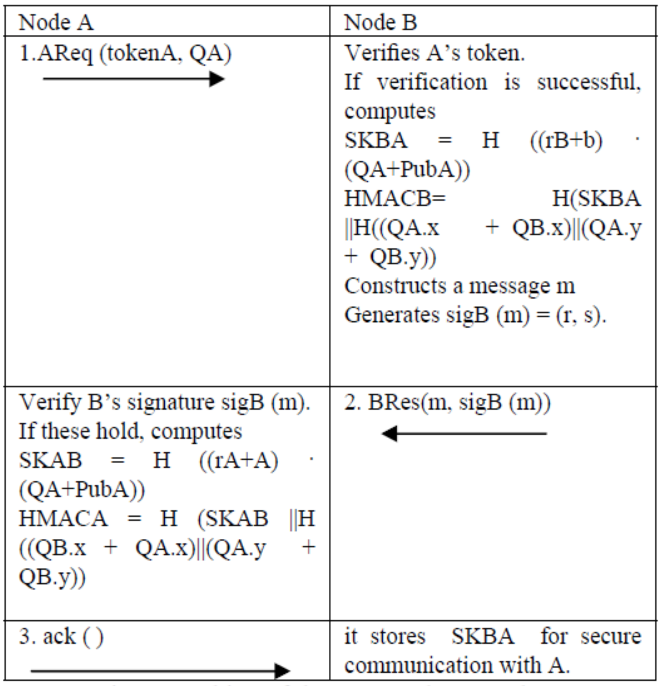
```
Algorithm AReq (tokenA, QA) {
If tokenA=tokenB then
Calculate SKBA using tokenB
Calculate HMACB using HMACB
Compute message m
Calculate sigB (m)
}
```

B. Authentication response message

```
Algorithm BRes (m, sigB (m)) {
Calculate SKAB using tokenA
Calculate HMACA using SKAB
}
```

C. Authentication acknowledgement message

```
Algorithm Ack ( ) {
Compare SKBA=SKAB
Compare HMACA=HMACB
If both conditions satisfy then node A and B are
authenticated
}
```



Node A	Node B
1.AReq (tokenA, QA) →	Verifies A's token. If verification is successful, computes SKBA = H ((rB+b) · (QA+PubA)) HMACB= H(SKBA ||H((QA.x + QB.x)||(QA.y + QB.y)) Constructs a message m Generates sigB (m) = (r, s).

Verify B's signature sigB (m).
If these hold, computes
SKAB = H ((rA+A) · (QA+PubA))
HMACA = H (SKAB ||H ((QB.x + QA.x)||(QA.y + QB.y))
	2. BRes(m, sigB (m))
	←

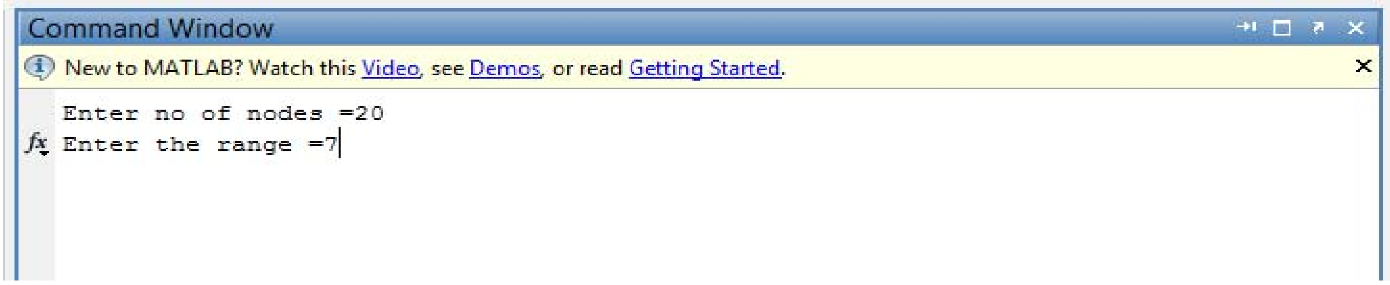
3. ack ( ) →	it stores SKBA for secure communication with A.

Figure 3.1: Working of Proposed work

The proposed protocol satisfies common security properties of a two party authenticated key agreement protocol such as known key security, perfect forward secrecy, key compromise impersonation resilience, unknown key share, implicit key agreement, key confirmation and explicit key confirmation. In the proposed protocol, key of confirmation is achieved at both communicating parties whereas in other protocols key confirmation is achieved at one end. Overall, we conclude that the proposed protocol is efficient compared with the existing protocols.

4. Simulation Results

The below figures show simulation results of the proposed work. It is made as user interface where user can enter the number of nodes and the communication range between the nodes and the red color in the figure shows the communication range of that vehicle's or the nodes and the blue color shows the authenticated nodes and the hash generated and the key given shown in the below figures.


Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
fx

```
Enter no of nodes =20
Enter the range =7
```

Figure 4.1: Entering number of nodes and range

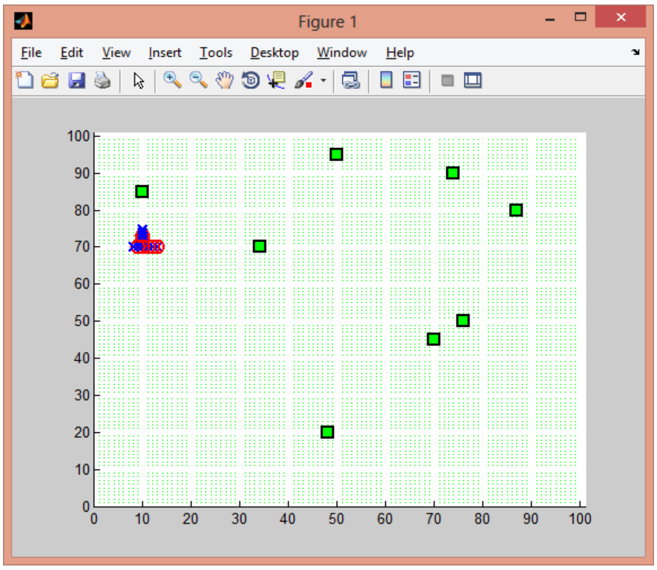


Figure 4.2: Two nodes in the range of communication

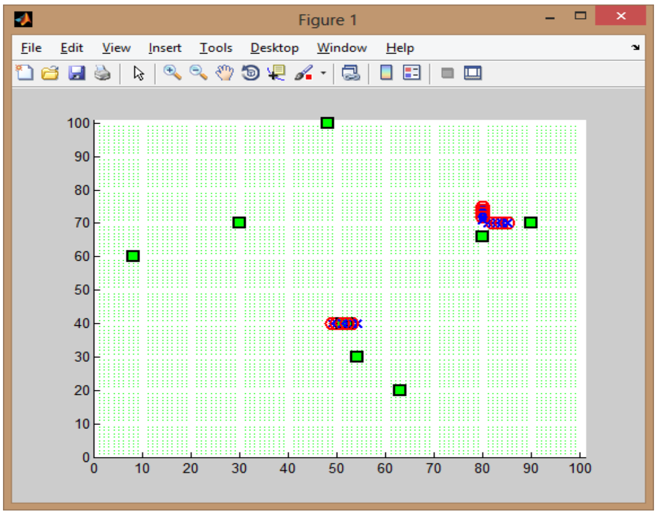


Figure 4.3: Case I Two pair of nodes in the range of communication

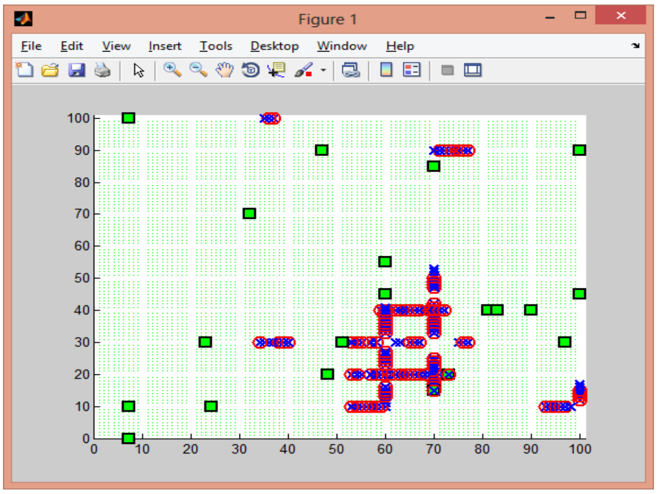


Figure 4.4: Case II Nodes in the range of Communication

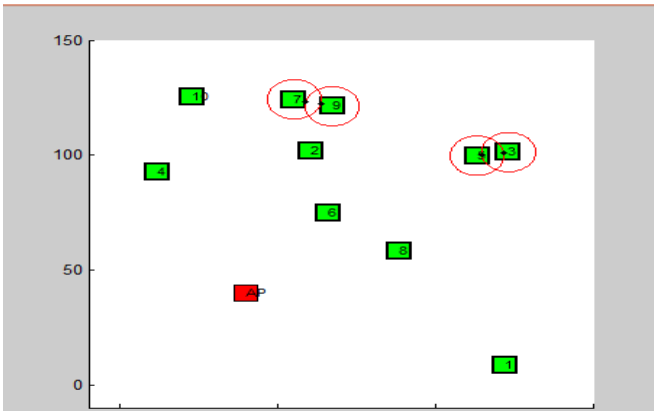
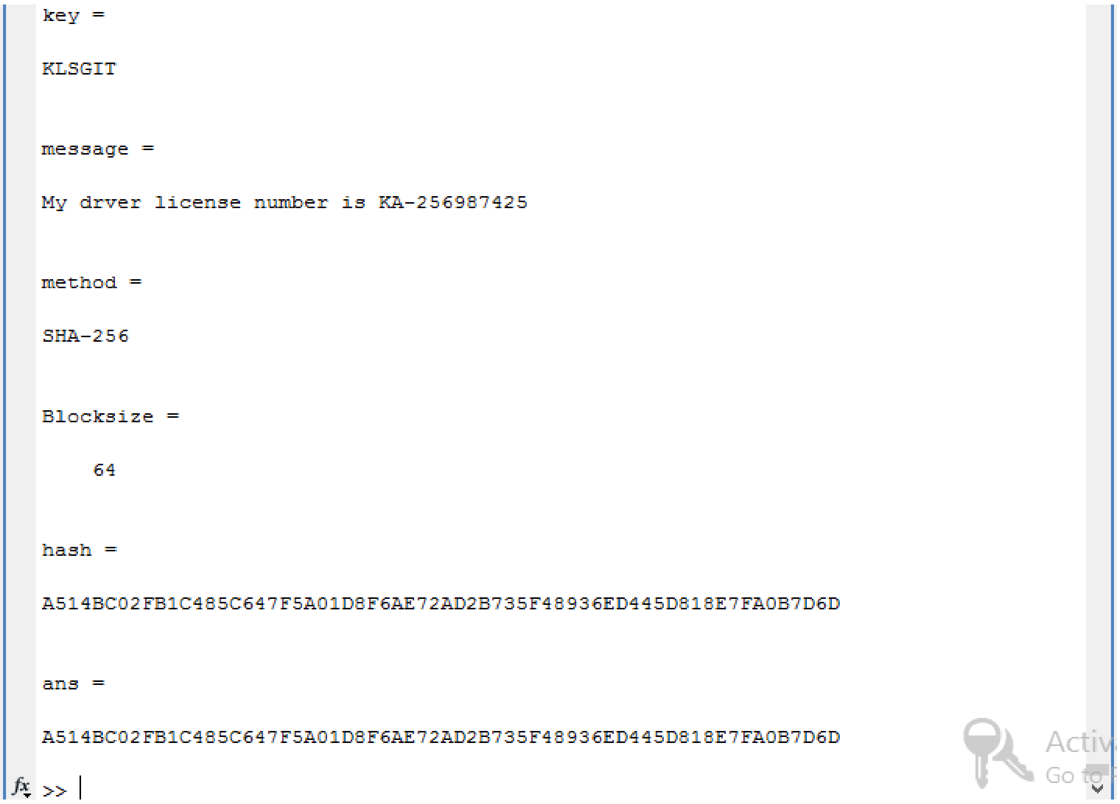
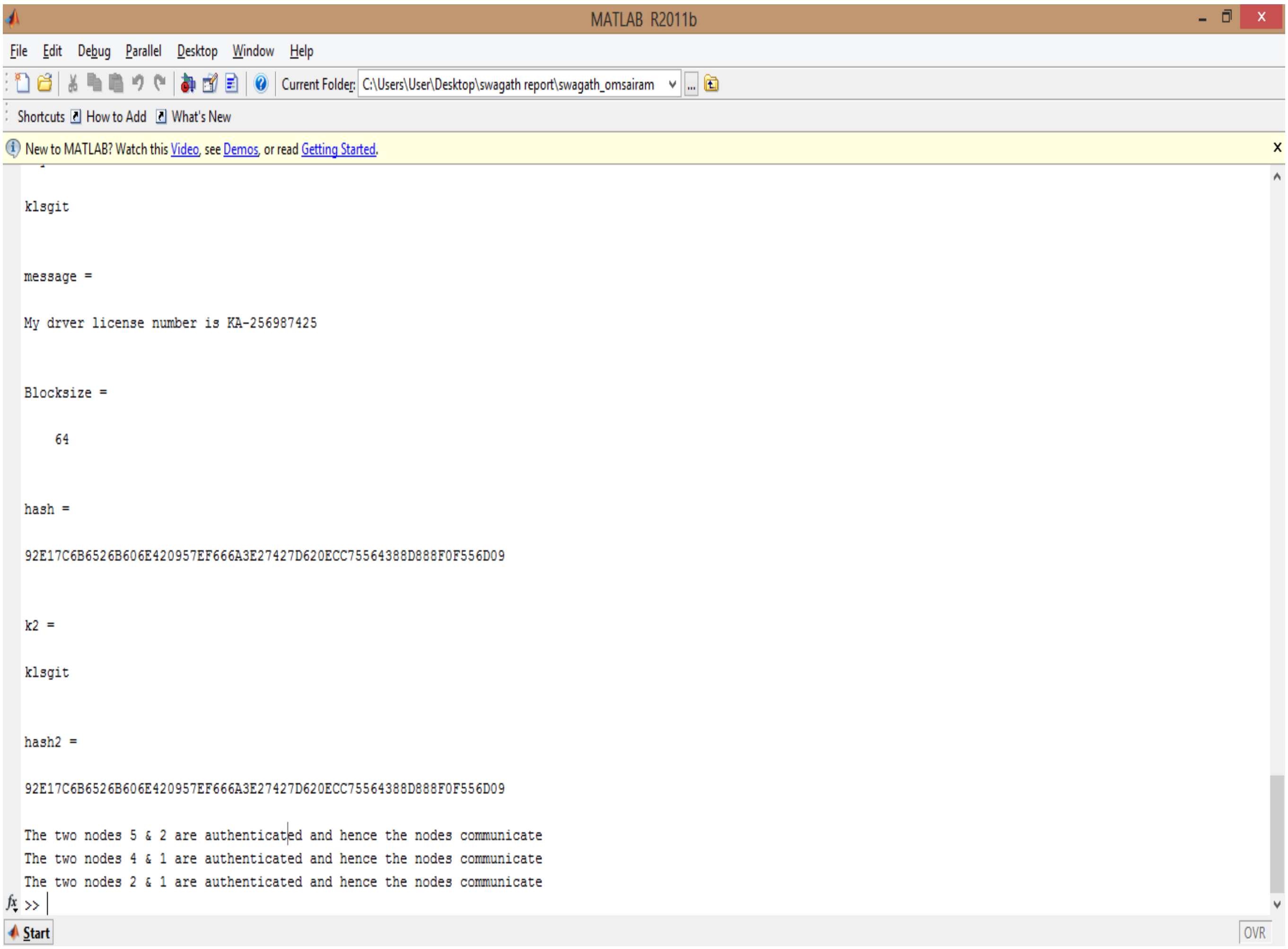


Figure 4.5: Authentication of nodes



```
key =

KLSGIT


message =

My drver license number is KA-256987425


method =

SHA-256


Blocksize =

    64


hash =

A514BC02FB1C485C647F5A01D8F6AE72AD2B735F48936ED445D818E7FA0B7D6D


ans =

A514BC02FB1C485C647F5A01D8F6AE72AD2B735F48936ED445D818E7FA0B7D6D

>> |
```

Figure 4.6: Hash message authentication



Current Folder: C:\Users\User\Desktop\swagath report\swagath_omsairam

New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
klsgit


message =

My drver license number is KA-256987425


Blocksize =

    64


hash =

92E17C6B6526B606E420957EF666A3E27427D620ECC75564388D888F0F556D09


k2 =

klsgit


hash2 =

92E17C6B6526B606E420957EF666A3E27427D620ECC75564388D888F0F556D09

The two nodes 5 & 2 are authenticated and hence the nodes communicate
The two nodes 4 & 1 are authenticated and hence the nodes communicate
The two nodes 2 & 1 are authenticated and hence the nodes communicate
>> |
```

Figure 4.7: The pair of nodes authenticated & in communication

5. Conclusion

In the VANET based proposed work a new cryptographic scheme for securing data from sender to a receiver by using HMAC based scheme is demonstrated. As compared to the conventional scheme the proposed scheme uses the text as the input data. The license is used as the anonymous credential which is kept to be confidential such that the impersonator cannot reveal the data unless and until he knows tha private key. The symmetric key mechanism is used in this proposed work. The work is simulated in MatLab environment which the results obtained are discussed with suitable images. However the data with the text is used where the text will be the vehicle owners name and address of his\her. The scheme achives less computation time for achieving compution of cryptographic actions.

In future, our work will consider investigating on hardware. The current work focusses using images with same size while in future the work will consider adopting the technique for different dimension of images and to evaluate practically the computation time with the conventional algorithms used for privacy preserved data transmission

Reference

[1] B. Corona, M. Nakano, H. Pérez, “Adaptive Watermarking Algorithm for Binary Image Watermarks”, *Lecture Notes in Computer Science, Springer, pp. 207-215, 2004.*

[2] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.

[3] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEE Proceedings -, vol. 152, pp. 561-574, 2005.

[4] F. Gonzalez and J. Hernandez, " A tutorial on Digital Watermarking ", In IEEE annual Carnahan conference on security technology, Spain, 1999.

[5] D. Kunder, "Multi-resolution Digital Watermarking Algorithms and Implications for Multimedia Signals", Ph.D. thesis, university of Toronto, Canada, 2001.

[6] J. Eggers, J. Su and B. Girod," Robustness of a Blind Image Watermarking Scheme", Proc. IEEE Int. Conf. on Image Proc., Vancouver, 2000.

[7] Barni M., Bartolini F., Piva A., Multichannel watermarking of color images, IEEE Transaction on Circuits and Systems of Video Technology 12(3) (2002) 142-156.

[8] Kundur D., Hatzinakos D., Towards robust logo watermarking using multiresolution image fusion, IEEE Transcations on Multimedia 6 (2004) 185-197.

[9] C.S. Lu, H.Y.M Liao, “Multipurpose watermarking for image authentication and protection,” *IEEE Transaction on Image Processing*, vol. 10, pp. 1579-1592, Oct. 2001.

[10] L. Ghouti, A. Bouridane, M.K. Ibrahim, and S. Boussakta, “Digital image watermarking using balanced multiwavelets”, *IEEE Trans. Signal Process.*, 2006, Vol. 54, No. 4, pp. 1519-1536.

[11] P. Tay and J. Havlicek, "Image Watermarking Using Wavelets", in *Proceedings of the 2002 IEEE*, pp. II.258 – II.261, 2002.

[12] P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.

[13] H. Daren, L. Jifuen,H. Jiwu, and L. Hongmei, "A DWT-Based Image Watermarking Algorithm", in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 429-432, 2001.

[14] C. Hsu and J. Wu, "Multi-resolution Watermarking for Digital Images", *IEEE Transactions on Circuits and Systems- II*, Vol. 45, No. 8, pp. 1097-1101, August 1998.

[15] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in *Proceedings of the 2003 IEEE TENCON*, pp. 935-938, 2003.