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 $1 \leq rA \leq q - 1$ 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 $1 \leq rB \leq q-1$ 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.

Figure 4.1: Entering number of nodes and range

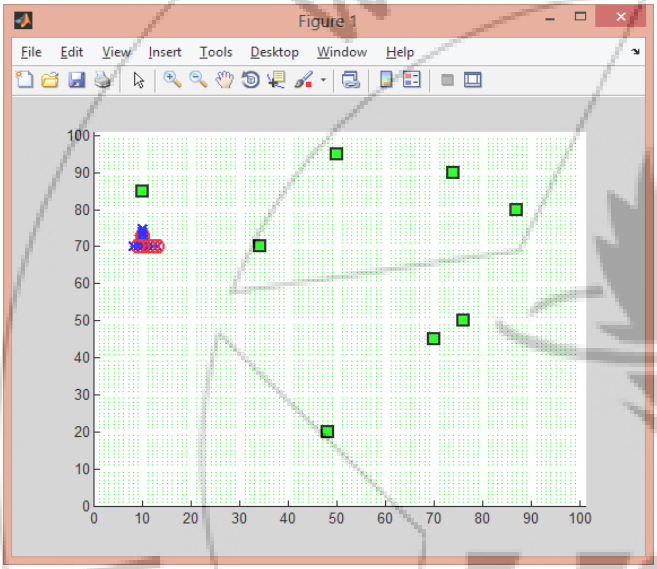

Figure 4.2: Two nodes in the range of communication

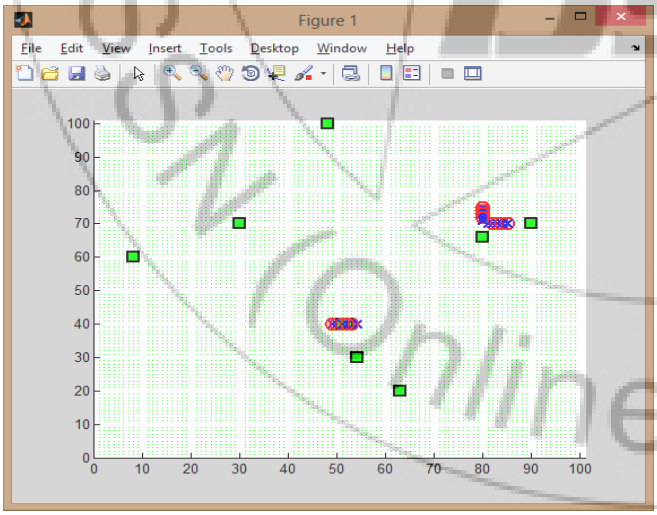

Figure 4.3: Case I Two pair of nodes in the range of communication

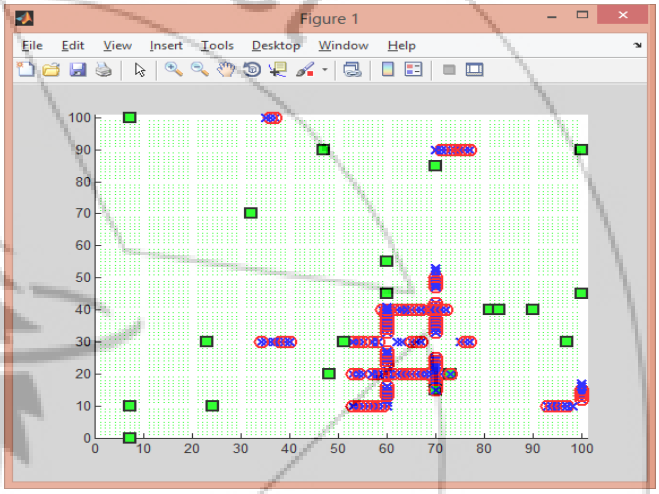

Figure 4.4: Case II Nodes in the range of Communication

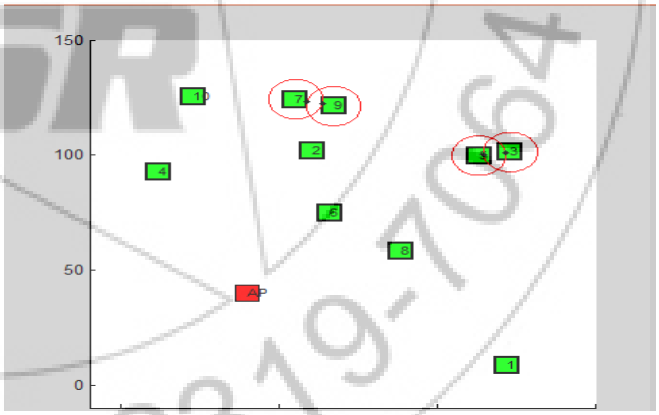

Figure 4.5: Authentication of nodes

```
key =

KLSGIT


message =

My drver license number is KA-256987425


method =

SHA-256


Blocksize =

    64


hash =

A514BC02FB1C485C647F5A01D8F6AE72AD2B735F48936ED445D818E7FA0B7D6D


ans =

A514BC02FB1C485C647F5A01D8F6AE72AD2B735F48936ED445D818E7FA0B7D6D

fx >>
```

Figure 4.6: Hash message authentication

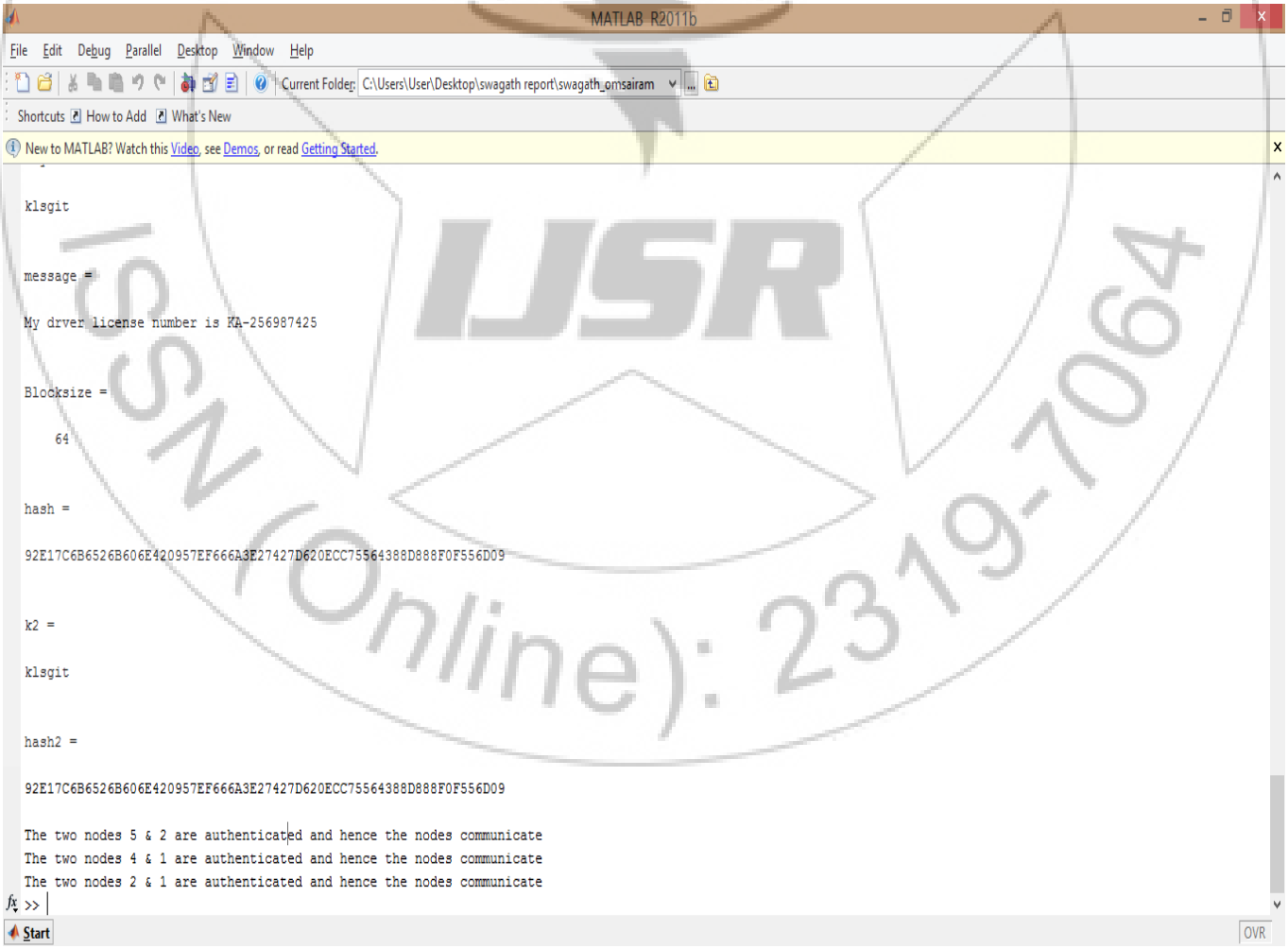

Figure 4.7: The pair of nodes authenticated & in communication

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.