ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 10(36), DOI: 10.17485/ijst/2017/v10i36/119184, September 2017* ISSN (Online) : 0974-5645

Enhancing the Security of Vehicle to Road Side Unit (RSU) Communication with Key Generation and Advanced Encryption Procedure in Vehicular Ad-Hoc Network (VANET)

Farheen Qazi[1], Fozia Hanif Khan[2*], Khurram Nawaz Kiani[3] and Sadiq Ali Khan[4]

[1]Department of Computer Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan; engr.fq@gmail.com
[2]Department of Mathematics, University of Karachi, Pakistan; ms_khans2011@hotmail.com
[3]Trafix LLC Karachi, Pakistan; kkiani@trafix.com
[4]Department of Computer Science, University of Karachi, Pakistan; msakhan@uok.edu.pk

Abstract

Traffic security using vehicle to road side unit communication has thrown many security challenges that should be overcome in order to achieve the security scenarios. VANET (Vehicular Ad-hoc Network) deals with the communication of vehicles as well as with the road side unit infrastructure for the multiple applications such as transit safety to deriver, public security, roadside facility locator, toll collection, traffic control and efficiency of freeway system. This is a type of mobile ad-Hoc network that uses the roadside equipment. This manuscript is intended to provide a secure protocol for the vehicular Ad-Hoc network for the roadside communication. The proposed study will not only generate the key as an orthogonal matrix with the very secure procedure, but also provided the new way of encryption and decryption procedure to enhance the communication between vehicle and road side unit. Instead of sending the key the receiver will generate the key by making the linear equation with the help of car registration number. The provided scheme will be beneficial for the real identity of the vehicles where security is major issue.

Keywords: Communication, Decryption, Encryption, Road Side Unit (RSU), Vehicular Ad-hoc Network (VANET)

1. Introduction

Vehicular Ad hoc Networks (VANETs) are the promising approach to provide safety and other applications to the drivers as well as passengers. "It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security in VANET got less attention. Now days, the sheer volume of road traffic affects the safety and efficiency of traffic environment. Approx 1.2 million people are killed each year on the road accidents. Road traffic safety has been the challenging issue in traffic management. One possible way is to provide the traffic information to the vehicles so that they can use them to analyze the traffic environment. It can be achieved by exchanging the information of traffic environment among vehicles. All the vehicles are mobile in nature, hence a mobile network is needed which can be self organized and capable of operating without infrastructure support as given in Figure 1. With the progress of microelectronics, it becomes possible to integrate node and network device into single unit and wireless interconnection, i.e. ad hoc network[1]".

2. Literature Review

Routing has been an intensive major research area in MANETs. AODV, DSD, DSR and OLSR[2] are node-centric

* *Author for correspondence*

MANET protocols in which topological end-to-end paths are created. "The solutions have been proposed to improve the VANET performance, which exploit the knowledge of relative velocities between nodes and the constrained movements of vehicles[3-5]. Geographical routing protocols, e.g., GPSR[6], GFG[7], and GOAFR[8], use node positions to route data between endpoints. Solutions proposed in[9] and[10] to improve recovery strategies in VANETs by either proactively detecting potential dead-end positions or using channel capabilities of wireless networks to decrease the number of hops on the recovery paths. The concept of anchor-based routing in sensor networks has been adapted to VANET environments. GSR[11] and SAR[12] integrate the road topologies in routing using those concepts. In these protocols, a source computes the shortest road-based path from its current position to the destination. To alleviate this issue, A-STAR[13] modifies GSR by giving preference to urban scenario served by transit buses each time a new intersection will be added to the source route. CAR[14] finds connected paths between source-destination pairs, considering vehicular traffic, and uses guards to adapt to movements of nodes. We note that real-life measurements with commercial GPS receivers[15] showed errors in the reporting of GPS positions in urban environments.

Xiaonan Liu in 2007[16] described an Intelligent Transport System (ITS) which can be used under the security pattern to provide the appropriate solving measures in concern with the security issues of VANETs from some aspects. Department for Transport in 2008[17] concluded that it had been seen from various studies that the number of lives lost in motor vehicle crashes worldwide every year is by far the highest among all the categories of accidental deaths. P.Caballero-Gil in 2009[18] analyzed the features of inter-vehicle and vehicle-to-roadside communications to propose differentiated services for node authentication, according to privacy and efficiency needs. Zuowen in 2010[19] proposed an improved privacy-preserving mutual authentication protocol for vehicle ad hoc networks by using secure identity-based group blind signature, the private encryption system and the public encryption system. Surabhi Mahajan in 2010[20] discussed a comparison between the two schemes that are used to reduce the overhead in authentication, when roaming - proxy re-encryption scheme and new proxy re encryption scheme. Hatem Hamad in 2010[21] proposed a new method of message security by using the coordinates in GPS (Global Positioning System) service".

3. Technical Challenges in Security of Vehicular Ad-hoc Network

"The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET. Some challenges are given below:

3.1 Network Management

Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as rapidly as the topology changed.

3.2 Congestion and Collision Control

The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

3.3 Environmental Impact

VANETs use the electromagnetic waves for communication.

These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

3.4 MAC Design

VANET generally use the shared medium to communicate hence the

MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

3.5 Security

As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied".

4. Methodology

The propose algorithm will provide the procedure for

the secure communication between the road side unit and the vehicle. The algorithm is based on the concept of generating orthogonal matrix which will be generated through the orthogonal line spanned by the unit vector[13]. The line which is orthogonal to the plane is basically a linear equation and this equation is participating in generating the orthogonal matrix. By the help of numeric and alphabetic values of the number plates of the car, linear equation will be first generated for the orthogonal matrix. The equation of plan for those vehicular IDs that contains zero digits will be generated in way that order of matrix will be reduced due to zero digits. The equation of plan will be generated only with non zero numeric values of vehicular IDs, which also reduces the order of matrix automatically.

The overall procedure for creating the key is as follows,

4.1 Key Generation Procedure

Generate the linear equation of plane by using the number plate of the car as follows:

Based on the total numeric and alphabetic values of the number plate the following equation can be generated as;

$$ax_1 + bx_2 + cx_3 + dx_4 + ex_5 + fx_6 = 0 \quad (1)$$

Therefore, $y = a^2+b^2+c^2++e^2+$

The orthogonal line L is spanned by the unit vector n = $\frac{1}{\sqrt{y}}(a, b, c, d, e, f)$

$V_1 = (1, 0, 0, 0, 0, 0)$

$V_2 = (0, 1\ 0, 0, 0, 0, 0)$

$V_3 = (0, 0, 1, 0, 0, 0)$

$V_4 = (0, 0, 0, 1, 0, 0)$

$V_5 = (0, 0, 0, 0, 1, 0)$

$V_6 = (0, 0, 0, 0, 0, 1)$

$$Tv_1 = (1, 0, 0, 0, 0, 0) - \frac{2a}{y}(a, b, c, d, e, f)$$

$$= (1, 0, 0, 0, 0, 0) - \left(\frac{2a^2}{y}, \frac{2ab}{y}, \frac{2ac}{y}, \frac{2ad}{y}, \frac{2ae}{y}, \frac{2af}{y},\right) \quad (2)$$

$$= \left(\frac{y-2a^2}{y}, -\frac{2ab}{y}, -\frac{2ac}{y}, -\frac{2ad}{y}, -\frac{2ae}{y}, -\frac{2af}{y},\right)$$

$$Tv_2 = (0, 1, 0, 0) - \frac{2b}{y}(a, b, c, d, e, f)$$

$$= (0, 1, 0, 0, 0, 0) - \left(\frac{2ab}{y}, \frac{2b^2}{y}, \frac{2bc}{y}, \frac{2bd}{y}, \frac{2be}{y}, \frac{2bf}{y},\right) \quad (3)$$

$$= \left(-\frac{2ab}{y}, \frac{y-b^2}{y}, -\frac{2bc}{y}, -\frac{2bd}{y}, -\frac{2be}{y}, -\frac{2bf}{y},\right)$$

$$Tv_3 = (0, 0, 1, 0, 0, 0) - \frac{2c}{y}(a, b, c, d, e, f)$$

$$= (0, 0, 1, 0, 0, 0) - \left(\frac{2ac}{y}, \frac{2bc}{y}, \frac{2c^2}{y}, \frac{2cd}{y}, \frac{2ce}{y}, \frac{2cf}{y},\right) \quad (4)$$

$$= \left(-\frac{2ac}{y}, -\frac{2bc}{y}, -\frac{y-2c^2}{y}, -\frac{2cd}{y}, -\frac{2ce}{y}, -\frac{2cf}{y},\right)$$

$$Tv_4 = (0, 0, 0, 1, 0, 0) - \frac{2d}{y}(a, b, c, d, e, f)$$

$$= (0, 0, 0, 1, 0, 0) - \left(\frac{2ad}{y}, \frac{2bd}{y}, \frac{2cd}{y}, \frac{2d^2}{y}, \frac{2de}{y}, \frac{2df}{y},\right) \quad (5)$$

$$= \left(-\frac{2ad}{y}, -\frac{2bd}{y}, -\frac{2cd}{y}, -\frac{y-2d^2}{y}, -\frac{2de}{y}, -\frac{2df}{y},\right)$$

$$Tv_5 = (0, 0, 0, 0, 1, 0) - \frac{2e}{y}(a, b, c, d, e, f)$$

$$= (0, 0, 0, 0, 1, 0) - \left(\frac{2ae}{y}, \frac{2be}{y}, \frac{2ce}{y}, \frac{2de}{y}, \frac{y-2e^2}{y}, \frac{2ef}{y},\right) \quad (6)$$

$$= \left(-\frac{2ae}{y}, -\frac{2be}{y}, -\frac{2ce}{y}, -\frac{2de}{y}, -\frac{y-2e^2}{y}, -\frac{2ef}{y},\right)$$

$$Tv_6 = (0, 0, 0, 0, 0, 1) - \frac{2f}{y}(a, b, c, d, e, f)$$

$$= (0, 0, 0, 0, 0, 1) - \left(\frac{2af}{y}, \frac{2bf}{y}, \frac{2cf}{y}, \frac{2df}{y}, \frac{2ef}{y}, \frac{2f^2}{y},\right) \quad (7)$$

$$= \left(-\frac{2af}{y}, -\frac{2bf}{y}, -\frac{2cf}{y}, -\frac{2df}{y}, -\frac{2ef}{y}, -\frac{y-2f^2}{y},\right)$$

By using the equation (2), (3), (4), (5), (6) and (7) generate the orthogonal matrix [13].

Step 1: By taking the mod of "y" we can able to find the multiplicative inverse which will be further used in key generation procedure. If multiplicative inverse in the mod 26 of "y" does not exist then calculate it for mod 7 then go for the mod 5 to get the multiplicative inverse in the initial state for the further procedure of the key generation.

Step 2: Generate the orthogonal matrix mentioned above and take it product with the multiplicative inverse as described in step # 01.

Step 3: The matrix which is obtained in step # 02 will be further simplified by taking corresponding mod value which initially selected in step # 01.

4.2 Encryption Procedure

Step 4: Initially generates the plaintext square matrix.

Step 5: Take the correspondently mod 26, mod 7 or mod 5 accordingly initially decided mod value in Step1.

Step 6: Take the transpose of the resultant matrix obtained from Step#05.
Step 7: For the further encryption take the product of key which K with the transposed matrix of plain text called P^T obtained in Step#06 as, $E = K * P^T$
Step 8: Take the respective mod of the resultant matrix obtained from Step # 07.
Step 9: Perform horizontal bit shifting of the first five rows to get the new matrix "E^{MH}".
Step 10: Perform vertical bit shifting of the first five columns to get the new matrix "E^{MHV}".
Step 11: Convert the newly obtained matrix from Step#10 into the alphabetic form to get the ciphertext.

4.3 Decryption Procedure

Step 12: Convert the alphabetic values in the form of numeric value to generate a matrix.
Step 13: Perform the reverse vertical bit shifting of first five columns of the matrix obtained from step # 12.
Step 14: Simply perform the reverse method of horizontal bit shift procedure.
Step 15: The matrix obtained in Step#14 will be further multiplied with key which is generated by predefined criteria, $D^M = K * E^M$. Where D^M is the decryption matrix.
Step 16: Take the respective mod of the matrix which is obtained in Step#15 further convert it in the form of alphabet to get the original text.

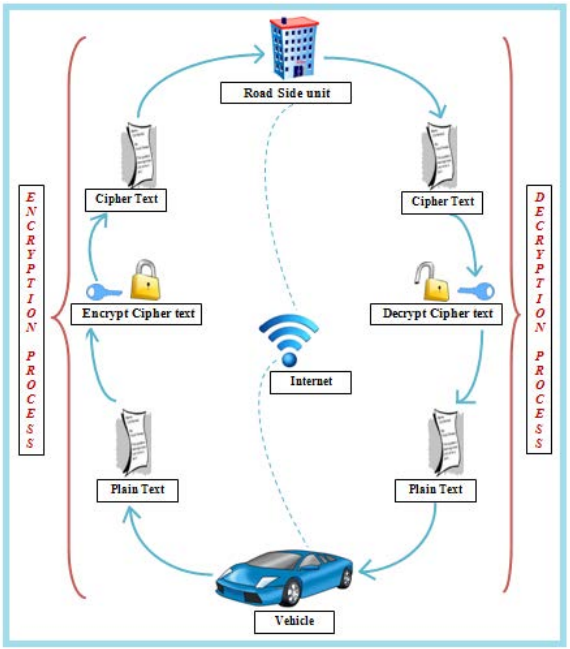

Figure 1. Vehicle-to-Road Side Unit (RSU) Communication.

5. Results and Discussion

In this paper, the different results have been evaluated using C-sharp simulator. The results shown indicate that the packet is sent between sender and receiver by using private key encryption algorithm. This means the same key is used for encryption and decryption. This leads to increase in throughput with reduce delay as shown in Table 1, where Figure 2 shows the comparison table between the block size and key generation time in milli sec.

We are considering three different vehicular IDs having distinct nature and made Evaluation to calculate the execution time having the file sizes 14, 26 and 42 bytes as showing by the Table 2. The comparison graph of Figure 3 indicates that the file size does not affect the execution time and not even on the condition that on which mode we are considering for the calculation.

The snapshoot shows the calculation of the proposed algorithm which has been generated on C-Sharp, and that also helps in concluding our results given by the Figure 4,

Table 1. Key generation time calculation of proposed algorithm

Block Size (n * n)	Key Generation Time Calculation (msec)
4 * 4	0.0027
5 * 5	0.0030
6 * 6	0.0031

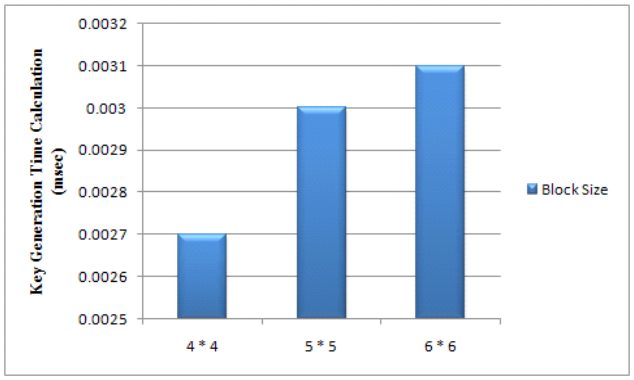

Figure 2. Comparison between the block size and the key generation execution time.

Table 2. Encryption and Decryption execution time of proposed algorithm

File Size (bytes)	Encryption & Decryption Execution Time (msec)		
	V_1 *(ID: AJW 853) Mod 5*	V_2 *(ID: APZ 162) Mod 7*	V_3 *(ID: AHX 767) Mod 26*
14	0.0188	0.0222	0.0224
26	0.0226	0.0226	0.0228
42	0.0231	0.0232	0.0232
Total: 82	**0.0645**	**0.068**	**0.0684**

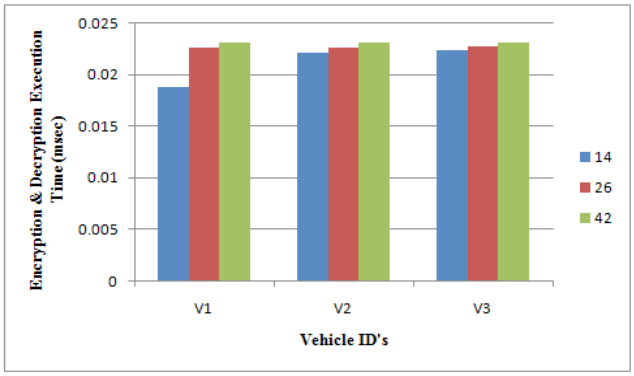

Figure 3. Encryption and decryption time in mili sec for 14, 26 and 42 bytes.

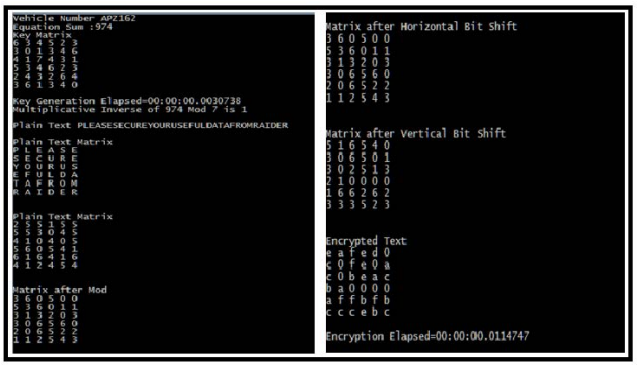

Figure 4. Snapshot of Result.

6. Conclusion

Security is basically provides the guarantees that the transmissions of data are authentic that is data is accessible only by authorized parties. The security techniques can be applied to vehicular users in Vehicular Ad-hoc Networks. The algorithm used in the paper is private key encryption in which sender and receiver communicate securely with the help of encryption key. The algorithm reduces delay, increases throughput, and provides authentication and higher security level in VANETs. The presented algorithm provides security over VANET, with end to end connectivity. The utility of the proposed technique is to send massages successfully between sender and receiver without any interruption. This algorithm is implemented for security, which is faster as well as secure than previously implemented algorithms.

7. References

1. Sesay S. Yang Z and Jianhua He. A survey on Mobile Ad Hoc Network. Information Technology Journal. 2004; 3(2):168-75.
2. Clausen T and Jacquet P. Optimized link state routing protocol (OLSR). Proceedings of IEEE - Intelligent Transport Systems. 2003.
3. Taleb T et. al. A stable routing protocol to support its services in vanets. IEEE Transactions on Vehicular Technology. 2007; 56(6):3337-47.
4. Hsu CH, Feng KT and Lu TE. Velocity-assisted predictive mobility and location - aware routing protocols for mobile ad hoc networks. IEEE Transactions on Vehicular Technology. 2008; 57(1):448-64.
5. Namboodiri V and Gao L. Prediction-based routing for vehicular ad hoc networks. IEEE Transactions on Vehicular Technology. 2007; 56(4):2332-45.
6. Karp B and Kung HT. GPSR: Greedy perimeter stateless routing for wireless networks. Boston, MA: Proceedings of the 6th Annual International MobiCom. 2000; p. 243-54.
7. Stojmenovic I, Bose P, Morin P and Urrutia J. Routing with guaranteed delivery in ad hoc wireless networks. ACM Wireless Networks. 2001; 7(6):609-16.
8. Y. Zhang F. Kuhn, R. Wattenhofer and A. Zollinger. Geometric ad hoc routing: Of theory and practice. Boston, MA: Proceedings of the 22nd Annual Symposium Principles Distributed Computing. 2003; p. 63-72.
9. K-F. et. al. Geographic forwarding with dead-end reduction in mobile ad hoc networks. IEEE Transactions on Vehicular Technology. 2008; 57(4):2375-86.
10. Zhao G, Ma X, Sun M-T and Liu X. An efficient path pruning algorithm for geographical routing in wireless networks. IEEE Transactions on Vehicular Technology. 2008; 57(4):2474-88.
11. Lochert C et. al. A routing strategy for vehicular ad hoc networks in city environments. Columbus, OH: Proceedings of the IEEE Intelligent Vehicles Symposium. 2003; p. 156-61.
12. Rothermel K, Tian J, Han L and Cseh C. Spatially aware packet routing for mobile ad hoc intervehicle radio networks. Proceedings of the IEEE Transactions on Intelligent Transportation Systems. Shanghai, China: 2003; 1546-51.
13. Khan FH, Shams R, Qazi F and Aaga DS. Hill cipher key generation algorithm by using orthogonal matrix. International Journal of Innovative Science and Modern Engineering (IJISME). 2015; 3(3):5-7.