International Journal of Security and Its Applications
Vol. 12, No. 1 (2018), pp.59-68
http://dx.doi.org/10.14257/ijsia.2018.12.1.05

Secure Identity-Based Cryptographic Approach for Vehicular Ah-hoc Networks

Sadiq Ali Khan[1], Fozia Hanif Khan[2], Farheen Qazi[3*],
Dur-e-shawar Agha[4] and Bhagwan Das[5]

[1]Department of Computer Science University of Karachi, Pakistan
[2]Department of Mathematics University of Karachi, Pakistan
[3,4]Department of Computer Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan
[5]Department of Electronic Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah. Pakistan
msakhan@uok.edu.pk, drfoizakhan@uok.edu.pk, engr.fq@gmail.com, engr.dureshawaragha@gmail.com, engr.bhagwandas@hotmail.com

Abstract

Now a day's year number of vehicles on the road has increased in recent years. "Potential threats and road accidents are increasing because to the high density of all these vehicles. In order to reduce these factors Wireless technology is designed to equip in-vehicle technology by sending messages to each other, known as vehicular ad hoc networks or VANET. The optimal goal of this research is to provide timely information to drivers and concerned authorities so that vehicular networks will contribute to safer and more efficient roads in the future. Thus to achieve the above mentioned goal, there is need for substantial research in the area of security for the possible deployment of VANET in near future. In terms of architecture, implementation of Identity Based Cryptography (IBC) schemes has been studied in order to provide better security and privacy for VANET, as it is considered as a viable choice due to the properties of VANET in comparison to the traditional Public Key Infrastructure (PKI) approach.

Keywords*: Encryption, decryption, cryptography, updated data (UPD), encrypted data (ENCD), final encrypted data (ENCDF), circular-left shift, circular-right shift, plain text, cipher text, key (KY)*

1. Introduction

In Wireless communication system, VANET is one of the hot topics that have been discussed widely by many researchers nowadays. It is known that VANET is a subset of MANET, where the nodes represent vehicles moving at high pace and it can be able to calculate the frequency of vehicular traffic [1]. Also it is used to provide safety, security and convenience to the automobile travelers and its can also be beneficial to warn the drivers for any possible collision that can occur on their way along with the automatic payments for the parking and for the toll collection *etc*. By this process communication between vehicles and nearby road-side infrastructure technology can be made possible and this whole procedure occurs because of the availability of wireless sensing device that has been installed in the vehicle [2]. New opportunities and related technologies such as commercial application for traffic congestion, accident control and weather updates have been emerged with the commencement of study on VANET [3]. But it must be known that; ad-hoc network does not based on centralized administration, and it does not depend

Received (July 9, 2017), Review Result (December 15, 2017), Accepted (January 12, 2018)

ISSN: 1738-9976 IJSIA

on any pre-established infrastructure due to the fact that the nodes are relying on each other for keeping the network connected. Although VANET is not a genuine ad hoc network since it does not rely on fixed infrastructure when vehicle-to-infrastructure communication occurs, but it uses the DSRC technology to connect the vehicle with the existing infrastructure [4].

Cryptography plays a major role to achieve security in any network, various types of encryption and decryption procedures are been developed to overcome the security issues [5]. But still all of them are not that much useful as they should because of the power constraints. Getting the high level security by using the simple computation is as difficult as to design successfully key management. Key management is the most important factor for any encryption key design procedure. Cumbersome algorithms does not provides guarantee to obtained high level security. Many advanced encryption algorithms, which are used for securing wireless networks, however, cannot be used in VANET, given that they have severe power constraints and resource constraints since they are small sensor devices residing on a vehicle [6].

The key generation scheme must also be computationally inexpensive yet secure. So it must be sufficiently complicated for making the communication more secure and authenticated. The proposed study will first generate the frame by using the vehicle information and perform the authentication for the data, then produce two keys KY1 and KY2 for the encryption and decryption procedure. This study will not only provides the encryption, decryption algorithm for VANET but also calculating the authentication code for the further key generation process by generating the frame which is based on 8 bits strings.

The study is organizes as follows, first section provides the introduction, previously developed techniques discusses in the second section, third section gives the working methodology of the algorithm along with the authentication code generation steps and with the steps of encryption and decryption of the proposed algorithm, section four mentions the results and simulations and finally the last section shows the conclusion and references.

2. Literature Review

There has been a rich literature on public-key management in VANET [7]. Few of them depends upon the certificate-based cryptography [8-11], and [12], which consider public-key certificates to authenticate public keys and binding public keys to the users' identities. The main idea behind using the Identity-based (ID-based) key management schemes, as they are simple key management procedures and reduced memory storage cost as compared to other cryptographic approaches. In ID based schemes the node or user identity, such as an IP address, is used to derive its public key, while the private key is generally provided by an external entity.

Another approach is used by [13], [14] which providing keying material through a web of trust. The technique in [15] employs hardware that integrates both asymmetric and symmetric cryptography modules for safety messaging and used hybrid approach that takes advantage of both asymmetric and symmetric cryptographic schemes. In [16] a technique is proposed as an essential complements to the passive mechanisms of encryption.

3. Methodology

The algorithm starts with the procedure of generating the frame which is used is authentication process. The base station will only receive the information of that automobile whose authentication code is matched; otherwise it will discard the data. The complete procedure of generating the frame is given by section 3.1. Once the authentication code for any vehicle is generated by frame then it will be further used in

key generation process and since the frame generation is complete random procedure therefore due to this randomness the resulting code will also be random and this will further effect keys generation process and make it more random, more secure and strong. In this study we generate two keys KY1 and KY2 by using the authentication based criteria. The reason for the generating the two keys is that in case of any intrusion or if one key is disclosed in anyway, the whole procedure will not be disclosed by anyone. More keys will make the procedures more secure.

3.1. Frame Generation

For the proposed algorithm we are generating the frame that helps in generating authentication code for any randomly selected automobile. The frame consists of 7-bit string, the first bit is called Authentication Code (AC), the second is randomly selected frame number, third one is the active bit whose data is recently updated (field will indicate the most updated vehicle information), on the fourth, fifth and sixth place we are considering the vehicle related messages which are road side unit to vehicle, vehicle to vehicle, vehicle to road side unit respectively, and in the end we have the current frame number that can be able to identify which data field is currently updated. Each encrypted data frame that is transmitted is appended with the sequence number of the reference frame used for generating the key, the field number in this reference frame whose value is used as the seed, and a sender authentication code. The proposed generated frame can be seen by the Figure 1.

Figure 1. Frame Format

AC= Authentication Code
RTV= RSU to Vehicle
VTV= Vehicle to Vehicle
VTR= Vehicle to RSU
CFN= Current Frame Number

3.2. Steps of Generating the Authentication (HVID)

1. Take the number plate of the vehicle as input ID which is based on numeric and alphabetic values.
2. Generation of the authentication code is based on Quadratic Formula.
3. Convert the alphabetic character into numbers by simply taking the cryptographic values of the English alphabets and add all of them. *e.g:* APZ-162, A+P+Z = (1+16+26)
4. Take the numeric part of the vehicle number plate and select its 1st and 3rd number.
5. Select constants of Quadratic equation a, b and c from step 3 and 4.
6. Choose the largest number as constant “b”, the second largest number selects as “c” and the smallest among all selects as “a”.
7. As a resultant we have two values and we choose positive value if it is an integer otherwise selects the negative value with the modulus. Take the square of the value obtain from step 6.
8. Hashed vehicle ID (HVID) is obtained by adding method of hash values obtained from step 7, HVID also called authentication code (AC).

3.3. Steps of Key Generation Algorithm

1. Key is the combination of AC and Active Bit by using the XOR operation; Key = AC $\oplus$ Active Bit. Where, the Active Bit is obtained from 3rd bit string of the randomly generated frame.
2. Convert the values of authentication code and active bit into binary form.
3. Applying XOR operation between AC and Active Bit.
4. Taking 2's complement of the output of step 3.
5. After taking 2's complement of the key perform one bit circular left shift.
6. Split the key into two halves as; KY1 and KY2.

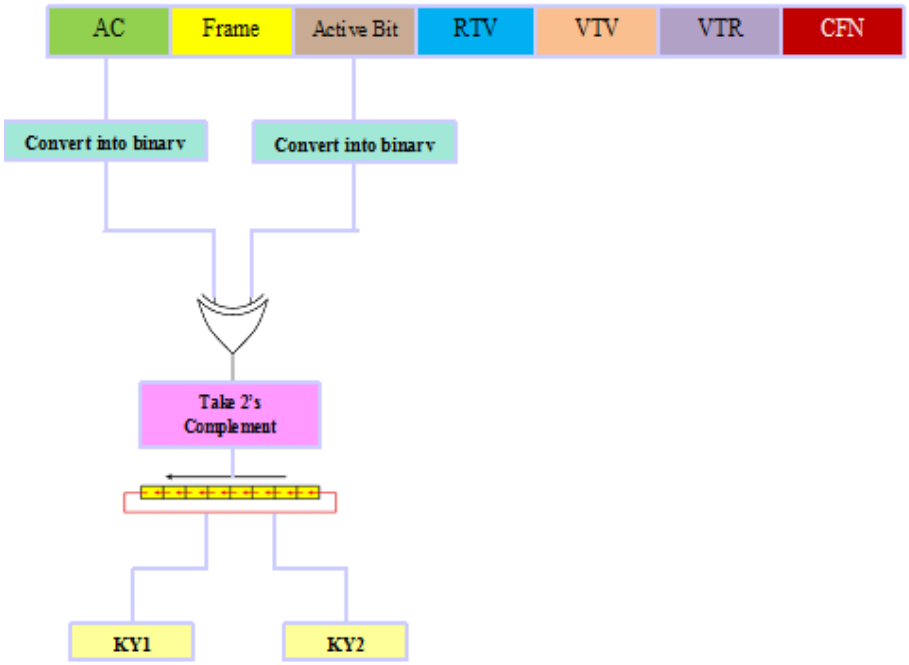

Figure 2. Design of Key Generation Process

3.4. Steps of Encryption Algorithm

1. Consider any random data related to RTV, VTV and VTR.
2. Obtained the binary value of the data coming from the step 1. Split the data obtained from step 2 into two halves called data 1 (DT1) and date 2 (DT2) respectively.
3. To obtained updated data 1 (UPD1), perform XOR operation between KY1 and DT2. For updated data 2 (UPD2) perform XOR operation between KY2 and DT1.
4. Concatenate UPD1 and UPD2 and obtain encrypted data (ENCD).
5. Apply 7-bit circular-left shift on ENCD and obtain the final encrypted data called ENCDF.
6. Complete procedure of encryption can be view in Figure 2.

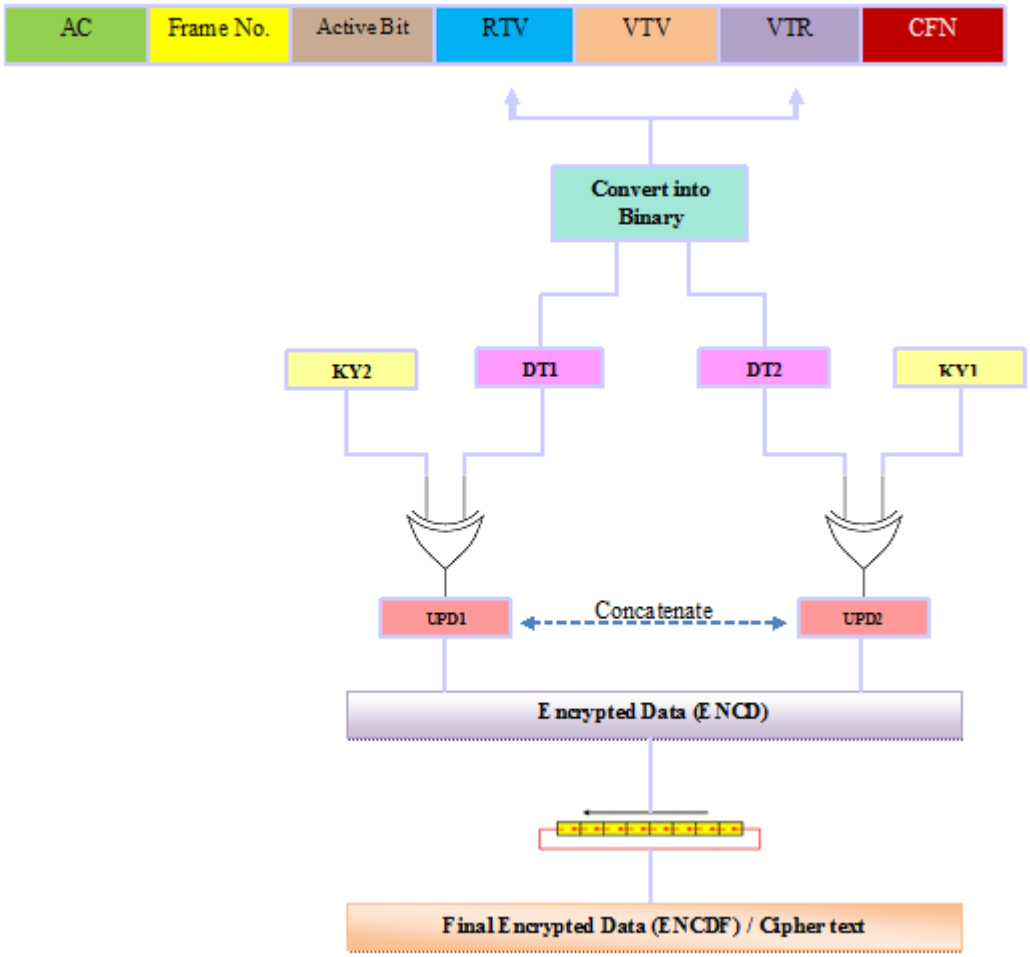

Figure 3. Design of Encryption Process

3.5. Steps of Decryption Algorithm

1. Before performing the decryption on data; first check the authenticity
2. After successful authentication operation applying 7-bit circular-right shift on ENCDF and get ENCD'.
3. Split ENCD' into two half UPD1' and UPD2'.
4. Apply XOR on KY1 with UPD2' and KY2 with UPD1', and obtain data DT1' and DT2'.
5. Concatenate the data DT1' and DT2' and get the original message.
6. Complete procedure of decryption can be view in Figure 3.

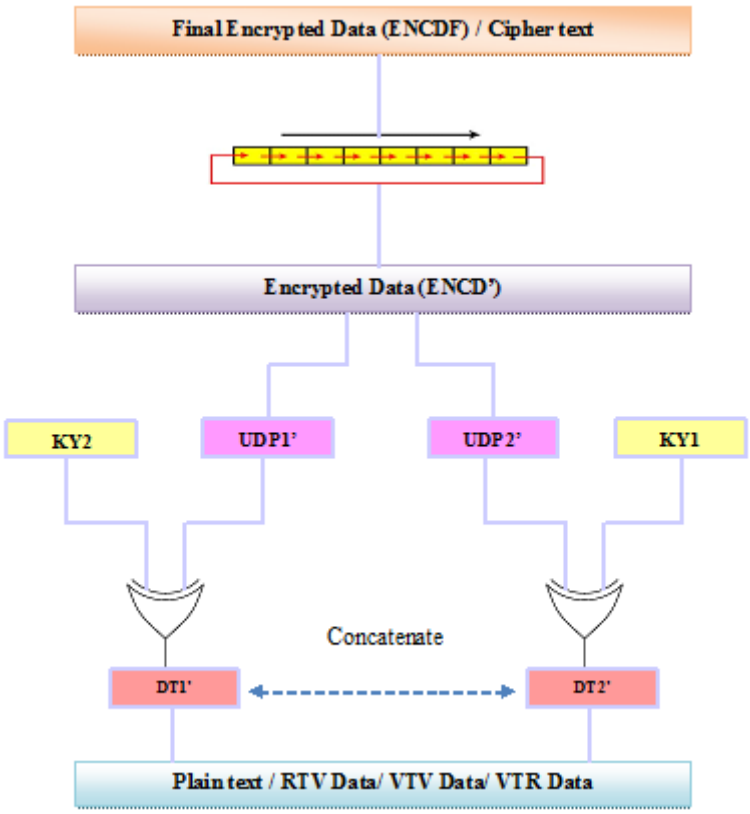

Figure 4. Design of Decryption Process

4. Results and Comparison

Performance of the proposed algorithm is analyzed in this section. As explained earlier the proposed algorithm is actually authentication based technique in which the frame will be generated for any specific vehicle which is a complete random procedure and after this a random authentication code will be created from the previously generated frame, due to this fact the key generation procedure is completely random as described in section 3.Because of this randomness of the whole procedure of key generation it can be easily seen from the Figure 4 that how the frame and key generation procedure is different from frame generation as far as the randomness is concerned these two are completely showing different scenario. In the Figure 5 the key generation time and authentication code time has been compared and showing their time differences. We have also made the comparison between the execution time of encryption and decryption procedures of the proposed algorithm with the existing algorithms given in [17]. According to the Figure 6, 7 it can be easily seen that the proposed algorithm showing better performance as far as the execution time is concerned. This is due to this fact that proposed technique is taking less computation operations instead of using the complicated operation but providing better security due to randomness of the procedure as given by Table 1, which is an actual requirement of the complete procedure since the VANET is based on temporary infrastructure with the help of less memory sensors therefore computation time will be less due to simple operations.

Table 1. Operations Performing In Provided Identity-based Security Algorithm

Operations	A.C	Key	Encryption	Decryption
XOR	1	1	2	2
2's Complement	-	1	-	-
Left Shift	-	1	7	-
Right Shift	-		-	7

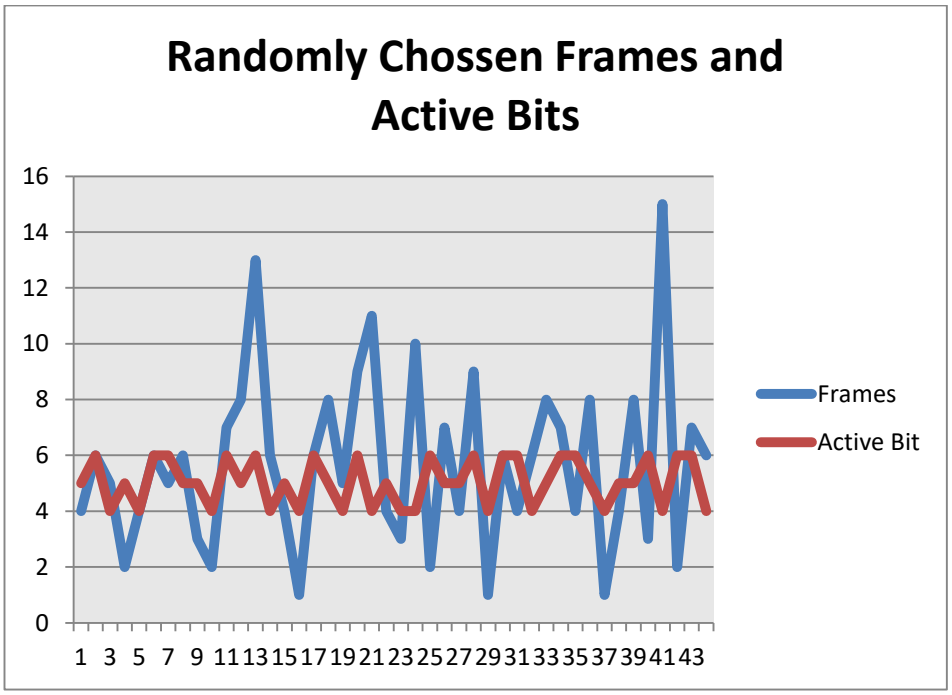

Figure 4. Presenting the Randomness in the Key Generation and AC Process

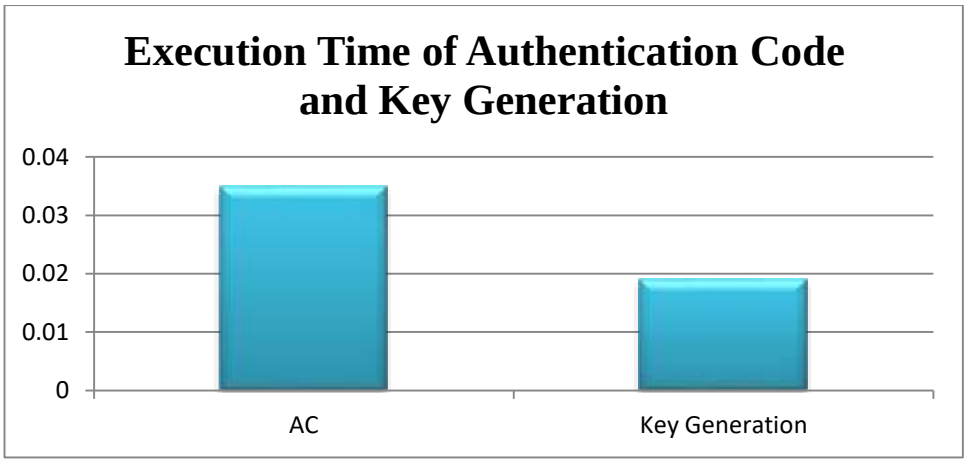

Figure 5. Execution Time of AC and Key Generation

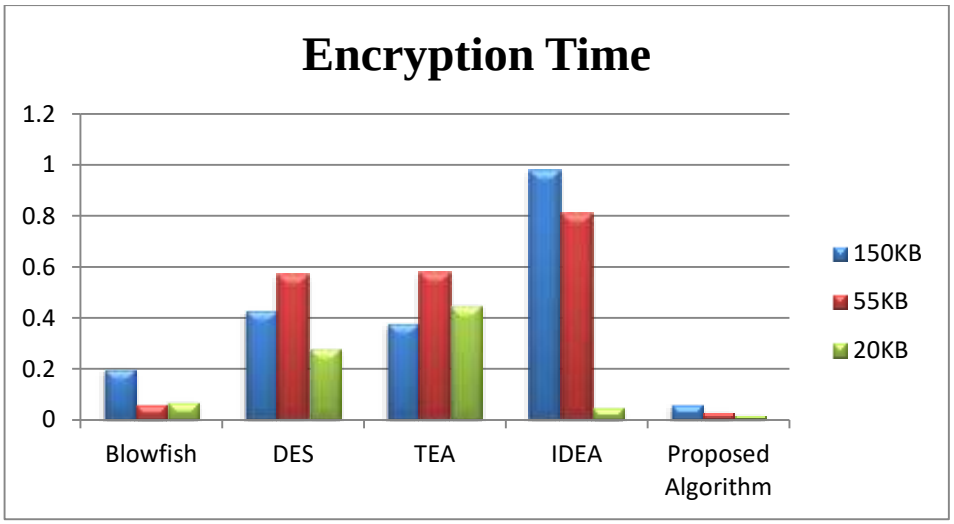

Figure 6. Encryption Time Comparison of Different Algorithm Between Different File Sizes

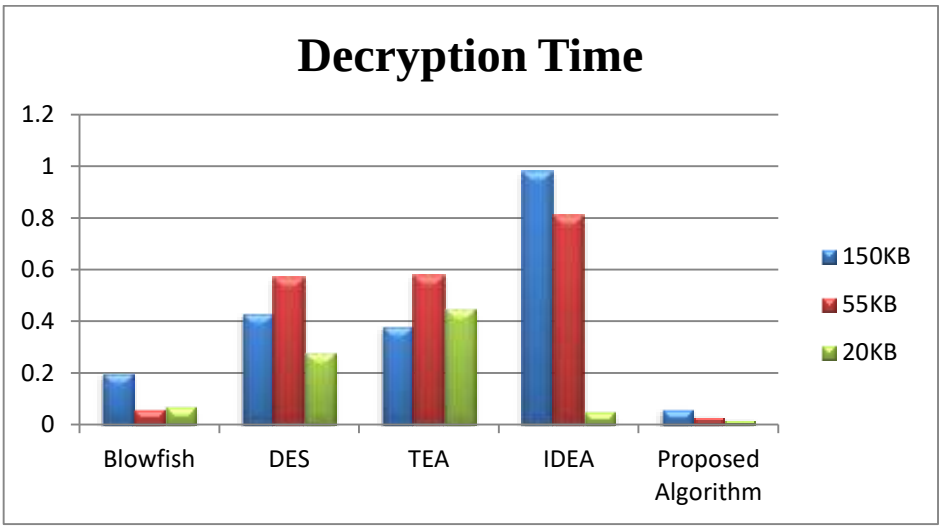

Figure 7. Decryption Time Comparison of Different Algorithm between Different File Sizes

5. Conclusion

VANET cryptographic authentication based algorithm has been presented by the above research and successful implementation and comparison has proved the validity of the proposed algorithm for execution time and randomness of key. The proposed study is first generating the authentication code by using the frame which is based on 7 bit string. The authentication code is further used in generating the two keys first are used in the data encryption and decryption procedures. The main idea of the above study is to provide better security by consuming less memory that is why the identity based research scheme has been implemented in VANET. The randomness of the key generated procedure plays main source for proving better security, the whole procedure of creating the authentication code and the key generation procedure is random based that's why it is more secure and more complicated. But due to less mathematical operations it is low memory consumption procedure also. As there is no strong infrastructure of VANET for the communication, therefore it should be as low memory consumption for the wireless sensor communication. The proposed study will be beneficial for the smart city applications.

References

[1] P. Sasikumar, C.Vivek and P.Jayakrishnan, "Key-Management Systems in Vehicular Ad-Hoc Networks", International Journal of Computer Applications (0975 – 8887), vol. 10, no.1, **(2010)**, pp. 23-28.
[2] L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Identitybased authenticated asymmetric group key agreement protocol", in Computing and Combinatorics, vol. 6196 of Lecture Notes in Computer Science, **(2010)**, pp. 510–519.
[3] M. Prabhakar, J. N. Singh and G. Mahadevan, "Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization", IEEE International Conference on Computer Communication and Informatics (ICCCI), **(2013)**, pp. 1-7.
[4] I. K. Azogu, M. T. Ferreira, J. A. Larcom and H. Liu, "A new antijamming strategy for VANET metrics directed security defense", IEEE Globecom Workshops (GC Wkshps) , **(2013)**, pp. 1344-1349.
[5] M.-F. Jhang and W. Liao, "Cooperative and opportunistic channel access for vehicle to roadside (V2R) communications", Mobile Networks and Applications, vol. 15, no. 1, **(2010)**, pp. 13–19.
[6] N. K. Chaubey, "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study International Journal of Security and Its Applications", http://dx.doi.org/10.14257/ijsia.2016.10.5.25, vol. 10, no. 5, **(2016)**, pp.261-274.
[7] T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li, "SPECS: secure and privacy enhancing communications schemes for VANETs", Ad Hoc Networks, vol. 9, no. 2, **(2011)**, pp. 189–203.
[8] X. Lin, R. Lu, C. Zhang, H. Zhu, P.H. Ho and X. Shen, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, vol. 46, no. 4, **(2008)**, pp. 88-95.
[9] N.-W. Lo and H.-C. Tsai, "Illusion Attack on VANET Applications", IEEE Globecom Workshops, **(2007)**, pp. 1–8.
[10] IEEE Std. 1609.2-2006, "IEEE Trial-Use Standard forWireless access in Vehicular Environments-Security Services for Applications and Management Messages", **(2006)**.
[11] P. Wohlmacher, "Digital Certificates: A Survey of Revocation Methods", Proc. ACM Wksp. Multimedia, Los Angeles, **(2000)**, pp.11–14.
[12] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks", J. Computer Security, Special Issue on Security, Ad Hoc and Sensor Networks, vol. 15, no. 1, **(2007)**,pp. 39– 68.
[13] B. Pradeep, M.M. Manohara Pai, M. Boussedjra and J. Mouzna, "Global Public Key Algorithm for secure location service in VANET", IEEE **(2009)**.
[14] P. S. L. M. Barreto, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps", Proc. Advances in Cryptology — ASIACRYPT, Taj Coromandel, Chennai, India, Dec. 2005, **(2005)**, pp. 515–32.
[15] P. Chowdhury, M. Tornatore, S. Sarkar, B. Mukherjee, A. A. Wagan, B. M. Mughal and H. Hasbullah, "VANET Security Framework for Trusted Grouping Using TPM Hardware", Second International Conference on Communication Software and Networks, (ICCSN '10), **(2010)**, pp. 309-312.
[16] M. Prabhakar, J. N. Singh and G. Mahadevan, "Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization", IEEE International Conference on Computer Communication and Informatics (ICCCI), **(2013)**, pp. 1-7.
[17] G. Sindhu and P. Krithika, "Analysis and comparison of symmetric key algorithms (Blowfish, DES, TEA, IDEA) in cryptography", IJSART, vol. 1, issue 11, **(2015)**, pp. 68-72.

Authors

M.Sadiq Ali Khan, he received his Ph.D Degree from KU in 2011 and his BS & MS Degree in Computer Engineering from SSUET in 1998 and 2003 respectively. Since 2003 he is serving Computer Science Department, University of Karachi as an Assistant Professor. He has about 18 years of teaching and research experience and his research areas includes Data Communication & Networks, Network Security, Cryptography issues and Security in Wireless Networks. He is the member of CSI, PEC, IEEE and NSP. He is currently Vice Chair IEEE Computer Society Karachi Section.

Fozia Hanif Khan, she is working as an Assistant Professor in the Department of Mathematics University of Karachi, Karachi, Pakistan. She has done her Ph.D. from University of Karachi University in Operations Research in 2012. Her fields of interest are cryptography, graph theory, Optimization Network Security and Wireless sensors Networks.

Farheen Qazi, she is a Ph. D Scholar (University of Karachi). She obtained her BS in Computer Engineering and MS in Computer Engineering (Specialization in Computer Networks) from Sir Syed University of Engineering and Technology, Karachi, Pakistan. Since 2008 she is working as a Lecturer in Department of Computer Engineering of Sir Syed University of Engineering and Technology, Karachi, Pakistan. Her research interests are Cryptography, Network Security, Artificial Intelligence and Wireless Sensor Network.

Dur-e-Shawar Agha, she is working as a Lecturer in the Department of Computer Engineering of Sir Syed University of Engineering and Technology, Karachi, Pakistan. She is a PhD scholar (University of Karachi) and did her BS in Computer Engineering and MS in Computer Engineering (Specialization in Computer Networks) from Sir Syed University of Engineering and Technology, Karachi, Pakistan. Her research interests are Cryptography, Artificial Intelligence and Wireless Sensor Network.

Bhagwan Das, he is working as a Lecturer in Department of Electronic Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Sindh, Pakistan.