|| Volume 2 || Issue 4 || OCTOBER 2017 || ISSN (Online) 2456-0774 ||
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Traditional Data Encryption Methods for VANET

Venkatamangarao Nampally[1], Dr. M. Raghavender Sharma[2], Dr. K. R. Balaji[3]
Department of Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, India
Department of Statistics, University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India
Department of Network Systems & Information Technology, Guindy Campus, University of Madras, Chennai, Tamil Nadu
n.venkat018@gmail.com[1], drmrsstatou@gmail.com[2] , balajicisl@yahoo.com[3]

***Abstract*— Encryption of information is a crucial achievement for VANET in order to reduce accidents & consequently improves traffic conditions to save lives. Security comes to information only when we provide encryption to information. Wireless communication is ubiquitous because of its flexibility to adapt to different scenarios. So authentication concept allows trusting both user and information, therefore, in order to increase the feasibility and better performance of cryptographic based protocols, we should have to investigate operation of different cryptography based methods.**

Keywords: *- VANETs, Encryption, Decryption, NIST, RSA, and Hash function.*

I INTRODUCTION

In this modern era manufacturers of vehicles equipped vehicles with secure hardware such that delivered data or information get easily encrypted. They are utilizing the dedicated short range communication (DSRC) to deliver information securely. VANET is collection of vehicle nodes with sensible sensors within it so that communicate with each other node. Sensitive information such as identity of vehicles and location privacy should be kept secret against unlawful tracing and user profiling; otherwise it is difficult to achieve secure communication among the vehicles in the network. ITS (intelligent Transport System) the family of IEEE 1609 standard defines achieving the security mechanism and the access to the physical layer for high speed and small distances for vehicular environments. Transmission of data or information among vehicle-to-vehicle exists through wireless medium in VANET. So there are chances of various attacks in VANET. Therefore encryption algorithms developed in order to deliver data securely.

VANET is a network of vehicles and infrastructure points. It consists of number of reliable sensors within it for communication. The primary goal of VANET is to provide road safety conditions to drivers as well as passengers. Figure 1 depicts a sensible message’s parts i.e. sending information to be delivered among vehicular nodes. In cryptography, Encryption means converting the normal text or plaintext containing raw materials into cipher text. Plaintext (also called clear text) is the text to be converted as unreadable form in encryption so that attackers cannot read information.

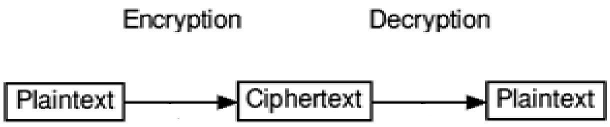

Figure 1: Encryption process

In order to read that encrypted data decryption is necessary in a cryptography algorithm. In an encryption process the intended information to be encrypted is called as plaintext.
In general, mostly we are using three types of data encryption algorithms are

- Symmetric or single key
- Asymmetric or double key(public key)
- Hashing
- Message authentication codes
- Digital signatures

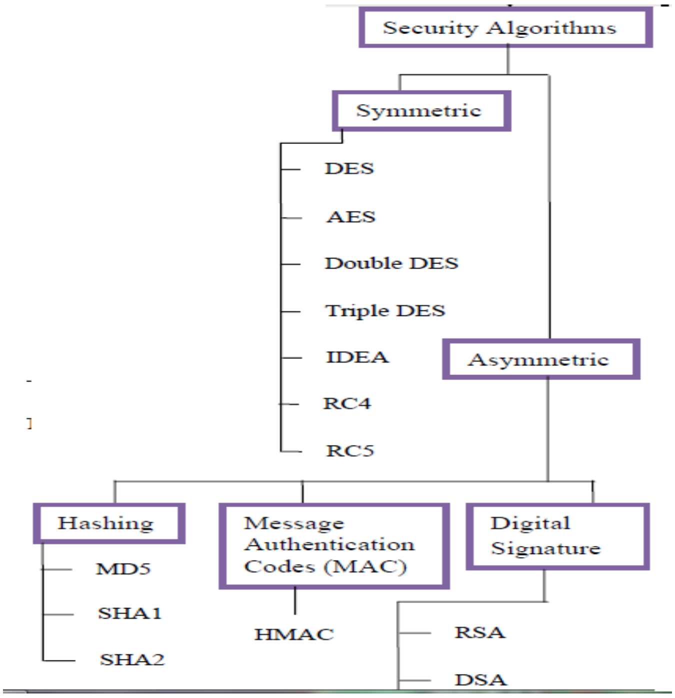

Figure 2: Security algorithms anatomy

This paper covers cryptography algorithms which are used mostly in VANET.

II RELATED WORK

Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri proposed a Short-lived Key Management scheme[1] which is used to solve the problems. Irfan Syamsuddina, Tharam Dillonb, Elizabeth Changc,and Song Hand [2] which is used to tackle the security and the privacy problems in RFID communications. Yong Hao[3] proposed A Distributed Key Management Framework With Co-operative Message Authentication in VANET which is to tackle the large computation overhead due to the group signature implementation . Edward David Moreno[4] proposed a system in which messages are exchanged in a secure way for VANET by using RSA, ECC and MQQ Algorithms. Saurabh Kumar Gaur [5] explained future security applications of VANET system. Uzma Khan et al. [6] presented a detailed survey on identified malicious nodes and cryptographic solutions. Digital signature is used for secure and reliable message communication and authentication [6]. Then R. Rivest explained for a solution to data encryption by using MD5 algorithm [7].

III METHODS

Most widely used different encryption algorithms today are as follows: Symmetric Algorithms, Asymmetric Algorithms, Hash Algorithms, and Message Authentication Code.

A. Symmetric Algorithms

A symmetric algorithm uses a single key to encrypt and decrypt the information. Here private key should be kept confidential because it is used to both encrypt and decrypt information and everyone with this key can read the encrypted document. Therefore, this method is called as the private key encryption method. A good symmetric algorithm provides integrity, availability, and confidentiality.

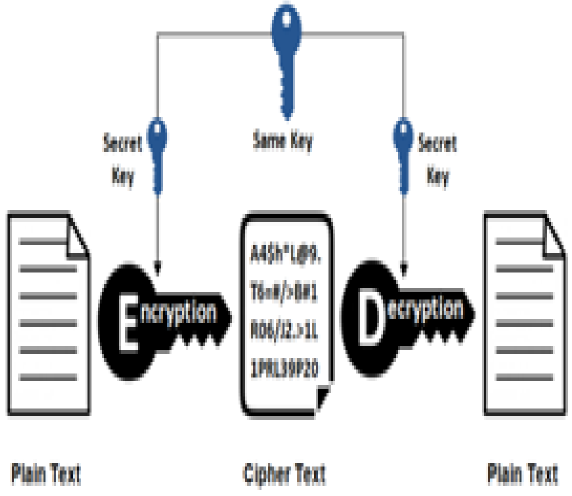

Figure 3: Process of single key encryption

There are several symmetric algorithms in use today. Some of globally recognized symmetric algorithms are: Advanced Encryption Standard (AES), Triple DES (3DES), and international data encryption algorithm (IDEA). Symmetric-key algorithms provide confidentiality, integrity, and availability.

B. Asymmetric Algorithms

An asymmetric algorithm uses two keys: one key is used for encryption and another for decryption which are mathematically related with each other. The public key is known globally. The private key should be protected and kept safe by the person who created it. The asymmetric algorithm is also known as public key cryptography. Asymmetric Algorithm uses more processing power and therefore is slower than the symmetric method. Asymmetric (public) key works in both directions. If a document is encrypted with a public key, it must be decrypted with the private key. For example, the person who creates an asymmetric key has the private key and has shares the public key with the person that he/she wishes to communicate with in secrecy. Asymmetric methods provide not only integrity, availability, and confidentiality but also authenticity, and non-repudiation. The authenticity and non-repudiation in the asymmetric method is accomplished by creating a digital signature, which can then be used to verify the sender and prevent the sender from denying the message. The sole ability for digital signature relies on asymmetric to work in both directions. Some good examples for asymmetric algorithms are Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman algorithm (DHA), and Elliptic Curve Digital Signature Algorithm (ECDSA). The most common asymmetric cryptography algorithm used today is RSA.

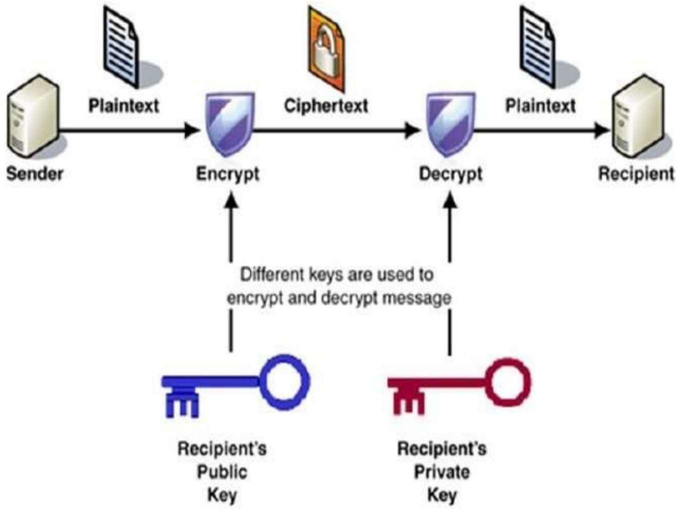

Figure 4: Working of Asymmetric key

C. Hash Algorithms

A hash function computes a fixed length output called the message digest from an input message of various lengths.

Hashing is used primarily to compare the digest of the original data with the digest of the current state of the data. Generally, a hash is used to create a unique digital fingerprint. The unique digital fingerprint is used to verify the content of a message/program has not been altered in transmission. It can be used on installed applications to create a unique digital fingerprint for each installed application. The digital fingerprint would be useful in the event that an attacker was successful at adding malicious code known as a program virus. The unique digital fingerprint is called a digest or sometimes a message digest or hash. One-way hash algorithm is used to reveal the original set of data i.e.it does not encrypt the data nor decrypt the data. If the data has not been compromised, the original digest and the current state digest will be identical. There are several hash algorithms in use today. Some examples for hash algorithms are: MD5, SHA family. It has been established that the hashing algorithm is a one-way algorithm that only provides integrity. It helps to prevent the spread of virus when used correctly, and is not a form that encrypts or decrypts data. It simply provides a digital digest to provide a way to know if the content of a message/program has been tampered with.

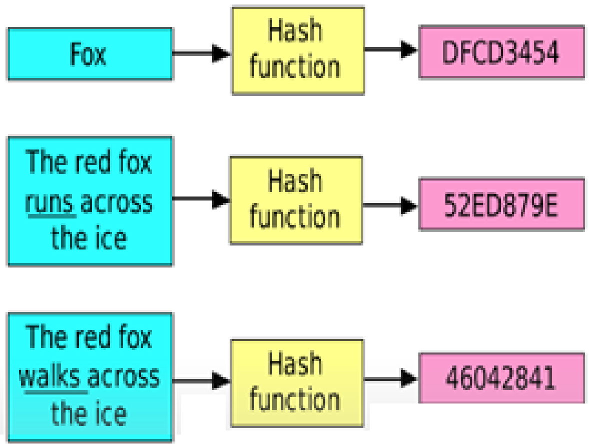

Figure 5: Working of a hash function

D. Message Authentication Code

Message authentication codes (MACs) are used to prevent the dissemination of unauthorized and corrupted message to avoid road accident in vehicular ad hoc network (VANET). MAC uses two inputs: a message and a secret key. Secret key allows the recipient of the message to verify the integrity of the message and authenticate that the sender of that message has the shared secret key or not. If a sender doesn't know the secret key, then resulted hash value is different, which tells the recipient that the obtained message was not from the original sender. There are four types of MACs available:

- Unconditionally secure
- Hash-function based
- Stream cipher-based and
- Block cipher based.

In the past, the most common way to create a MAC was using block ciphers, but now-a-days Hash-based MACs (HMACs) which use a secret key to produce a hash value are used widely. HMAC provides data integrity and authentication simultaneously.

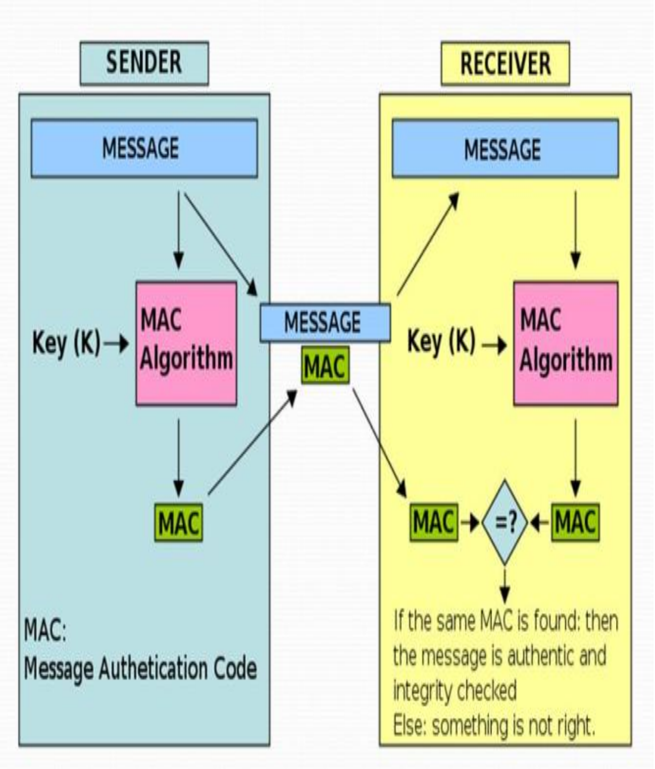
SENDER
RECEIVER
MESSAGE
MESSAGE
Key (K)
MAC Algorithm
MESSAGE
MAC
Key (K)
MAC Algorithm
MAC
MAC
=?
MAC
MAC:
Message Authetication Code
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Figure 6: Working of a MAC algorithm

IV CONCLUSON

It is expected that the differences among the data encryption algorithms in use today have been learned, along with how to choose the best one to use in a given situation. The reader also learned that the longer the key the less chance of collision and the more secure the hash algorithm is. In addition, the NIST has recommended that SHA-2 and above be used, and is considered a secure hash algorithm. Furthermore, it was learned that symmetric is much faster than asymmetric. Hence, Group encryption key-management schemes for a VANET have been performed. There is a considerable improvement in the data communication between the nodes after key management techniques have been employed. This technique can be used in security-sensitive applications like police and government agencies where VANETs are increasingly being used. We can achieve the security from modification and provides protection against fabrication and modification attacks by using encryption methods.

ACKNOWLEDGMENT

I will be thankful forever to the LORD BAJARANGBALI for his boundless blessings showered on me. I am very grateful and express my heartfelt countless Namaste to most respectable person who are Dr. S. Ananthi madam ji,B.E.,M.Tech.(IISC),Ph.D., Associate Professor, Department of Network Systems and Information Technology, University of Madras, Guindy Campus, Chennai for their constant support, invaluable help to the progress of my paper work. I would like to express my heartfelt special thanks to most respectable, emeritus and senior Prof. (ret.) Dr.K.Padmanabhan, Former Head, CISL and Emeritus Professor in AC Technology College, Anna University. I would like to express special thanks to Prof. (ret.) Ramana Murthy M. V., Department of Mathematics & Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, and Prof. (ret.) Shankar B., Department of Mathematics, University College of Science, Osmania University, Hyderabad, Telangana and Radhakrishna Peddiraju sir for clarifying my doubts. I take this opportunity to express my heartfelt thanks to Dr. K.R.Balaji M.Sc.,M.Phil.,Ph.D. Department of NS & IT, University of Madras, Guindy Campus, Chennai, and Arun Ananthanarayanan, UGC research scholar, Department of NS & IT, University of Madras, Guindy Campus, Chennai for giving their constant support and valuable help.

REFERENCES

[1] Short-lived Key Management for Secure Communications in VANETs Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri Wireless Ad hoc and Sensor Networks (WASN) Laboratory Department of Information Engineering, University of Parma, Italy, 2011.

[2] A Survey of RFID Authentication Protocols Based on Hash-Chain Method Irfan Syamsuddina, Tharam Dillonb, Elizabeth Changc, and Song Hand *aState Polytechnic of Ujung Pandang, Indonesia b,c,dDEBI Institute, Curtin University of Technology, Australia* , 2008

[3] A Distributed Key Management Framework with Cooperative Message Authentication in VANETs , Yong Hao, *Student Member, IEEE*, Yu Cheng, *Senior Member, IEEE*, Chi Zhou, *Senior Member, IEEE*, and Wei Song MARCH 2011.

[4] Edward David Moreno, Leila C.M. Buarque, Florêncio Natan, Gustavo Quirino and Ricardo Salgueiro "“Impact of Asymmetric Encryption Algorithms in a VANET”.

[5] Saurabh Kumar Gaur, S.K.Tyagi and Pushpender Singh, "“VANET System for Vehicular Security Applications", International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, No.6, 2013.

[6] R. Engoulou, “Securisation des vanets par reputation des noeuds “, thesis report, Ecole Polytechnique de Montreal, **2013**.

[7] R. Rivest, “The MD5 Message-Digest Algorithm,” RFC 1321, Apr. 1992.

[8] https://www.researchgate.net/publication/274173982_Security_Challenges_Issues_and_Their_Solutions_F or_Vanet [Last Accessed on 17-oct-2016]

[9] http://blog.tanyakhovanova.com/2010/11/one-way-functions/

[10] http://cdn.intechopen.com/pdfs-m/12879.pdf

[11] https://www.tutorialspoint.com/cryptography/images/public_key_cryptography.jpg

BIOGRAPHY

Dr. M. Raghavender Sharma (drmrsstatou@gmail.com) pursed Bachelor of Science in Mathematics, Master of Science in Statistics, and achieved Doctoral Degree in Statistics, all degrees from Osmania University, Hyderabad, Telangana, India, and currently he is working as an Assistant Professor and Head of Department, Department of Statistics at University College of Science, Saifabad, Osmania University, Hyderabad, Telangana, India. He is supervising many Ph. D.’s. He has excellent teaching track record with 25 years teaching experience.

Dr. K. R. Balaji (balajicisl@yahoo.com) has completed M.sc, M.Phil., Ph.D. currently he is working at University of Madras, Guindy Campus, Chennai, Tamil Nadu, India in the department of network systems & information technology. He has presented papers at the National and Interactional conferences relating to convolutional encoding and fuzzy based decoding as alternative to Viterbi’s decoder. His special interests are in Telecommunication Engineering and Mobile wireless sensor networks

Mr. Venkatamangarao Nampally (n.venkat018@gmail.com) pursed Bachelor of Science in Computer Science, Master of Science in Computer Science and Master of Technology in Computer Science & Engineering, all degrees from Osmania University, Hyderabad, Telangana, India, and pursed Master of Philosophy from University of madras, Chennai, Tamil Nadu, India. His main research work focuses on VANET communication. He has 7 years of teaching experience and 2 year of Research Experience.