Indonesian Journal of Electrical Engineering and Computer Science
Vol. 14, No. 3, June 2019, pp. 1425~1432
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i3.pp1425-1432

A chaotic based Integrity verification and encryption model for real-time VANET

Kareemulla Shaik, Md. Ali Hussain
KLEF Guntur Andhra Pradesh, India

Article Info

Article history:

Received Oct 14, 2018
Revised Nov 17, 2018
Accepted Feb 27, 2019

Keywords:

Chaotic maps
Encryption model
Integrity verification
VANET security

ABSTRACT

Integrity and data privacy are the main security parameters between the vehicle and roadside unit (RSU) over large VANETs. The integrity of the vehicle is used to check its identity against the neighboring nodes, whereas data privacy ensures that the data of a vehicle has not been altered during the communication process. VANETs provide vehicles to give information about the security parameters and identity to vehicle to infrastructure communication and vehicle to vehicle communication. Most of the traditional VANETs are vulnerable to data security, integrity and authentication due to change in dynamic topology. Also, Traditional security models require limited data size for data security between the V2V or V2I. In this paper, an integrity verification model and non-linear double encryption model were proposed and implemented on large geographical VANET map. The main objective of the proposed model is to improve the security of the V2V communication in large VANETs. Experimental results proved that the proposed security model has less computation cost for encryption model and higher bit change during integrity verification compared to the existing approaches

Corresponding Author:

Kareemulla Shaik,
KLEF Guntur Andhra Pradesh,
Lecturer, Mazoon College, Muscat Oman, India.
Email: kareem.mtech@gmail.com

1. INTRODUCTION

T VANET's are self-organized networks with dynamically changing topology over wireless communication. Communication in VANET can be classified as "Vehicle to Vehicle" (V2V), "Vehicle to Infrastructure" (V2I) or Hybrid Communication.

VANET consists of a trusted authority (TA), road units (RSU) and vehicles with embedded units (OBUs) as essential authentication units. The functionality of the VANET is autonomous decentralization for mobility-adaptive operation. Such a wireless network is self-organizing and does not necessarily depend on a pre-existing infrastructure.

In recent years, VANET has gained much attention due to its probable contribution towards effective solutions for dealing with traffic related problems and saving the lives of pedestrians, drivers, and passengers on the road. It transforms every vehicle into a wireless node so that each of them can connect within 100 to 300 meters range for exchanging data. Due to this mobility, VANET is vulnerable to physical threats that trigger probable vulnerabilities for promising attackers. The communication must be facilitated through the connection of fixed roadside unit (RSU) to the network's backbone. The communication protocol determines the distribution of the RSU, e.g. some protocols require the region borders to have roadside units, others require the intersections to have the units, and others require the whole road network to have an even distribution.

Most of the research works have been implemented on static attacks in public-key approaches, symmetric key approaches, hybrid approaches, and ID-based cryptography. However, to perform message authentication, traditional models used non-interactive, identity-based digital signature algorithms, the unidirectional hash chain, and the elliptic curve. Authentication is the key condition for the safety of vehicle communication. In the Public Key Infrastructure (PKI), the Certificate Authority (CA) is responsible for providing the vehicles with a pair of public/private keys and a certificate. This system does not support privacy. To support PKI-related privacy issues, the vehicle must be preloaded with multiple public / private key pairs and certificates. In symmetric key schemes, symmetry is created that is shared between the vehicle and the RSU. The verification of messages on the sender side depends on the authenticity which is sent by RSU.

Papapanagiotou et al. [1] implemented an authorization and authentication in VANETs using a distributed version of OCSP in their certificate validation. However, they ignored the privacy issues. Blum &Eskandarian et.al. [2] developed a security architecture for VANET with the use of a Public key infrastructure (PKI) and a virtual infrastructure where cluster-heads are responsible for reliably disseminating messages by a sequential unicast instead of broadcast. The approach creates bottlenecks at cluster-heads in addition to high-security overhead. Gerlach et.al, presented a novel architecture to integrate trust and privacy services for the use in vehicular environments. Zhu et.al, [3] have dealt with the challenges, adversary types and some attacks encountered in vehicular networks. They also described several security mechanisms that can be useful in securing these networks.

In [4], a novel approach is proposed to countermeasure the false public key certification in the form of a certification system for message authentication in VANETs. In this model, they used a decentralized system under the supervision of a root authority. This helps to make the authentication service more reliable. Lu et al [5] proposed the security of vehicular communication using an ECPP (Efficient Conditional Privacy Preservation) protocol. The authentication of anonymous messages is designed using a PKI signature scheme.

Shen and Wasef's [6] proposed the aggregated signatures and certificate verification scheme to enhance the integrity of the OBU's to verify the public keys and the signatures on the sender's certificate simultaneously. The messages sent by vehicles are authenticated using hash operations and the Message Authentication Code in the model proposed by Jiang et al [7]. They used a novel message signing operation using the two-level key hash chains.

In [8], Horng et al. proposed a SPECS (Security and Privacy Enhancing Communication Schemes) model on VANETs. The Security and Privacy Enhancing Communication Scheme is used to filter the valid signatures from the invalid signatures using the batch binary search. SPECS have been improved in the same context by Horng et al. in their protocol, b-SPECS+, which prevents impersonation attacks. Here, the nearby RSU verifies the signature of each vehicle and broadcast the attack notification to other vehicles in the network.

Bilinear pairings are utilized to construct ID-based cryptosystem wherein the encryption scheme instantly results in a public key mechanism. However, bilinear pairings have their own limitations when it comes to computation time and level of difficulty. These operations are costlier than other cryptographic primitives[9], [10].

The main contribution of the paper includes:

a) A novel vehicle integrity verification model with dynamic chaotic parameters is implemented on VANETs.
b) A novel double encryption model for strong data security is implemented in VANETs.

2. RESEARCH METHOD

Vehicle(OBU): Each vehicle must be registered by TA with the parameters of the public key and the corresponding private key.

RSU: RSU is a stationary sub-state unit that has a wireless access point, secure memory storage, and computational capabilities.

TA: TA records OBU and RSU. It initializes them with information about the public key or private keys.

Notations used in this paper as shown in Table 1.

Table 1. Notations Used in this Paper

Notations	Description
$T_n(x)$	Proposed Chaotic Map
$Z(n^2,*)$	Multiplicative group
P(x)	Polynomial space
s(k)	Secret key
g1 and g2	Random group elements
M	Message
Pubk	Public key
C1(x)	Cipher text 1
C2(x)	Cipher text 2
H	Hash Value Generated

In the proposed model, many vehicles and routes are considered for vehicle identity verification against malicious vehicles. The nodes are dynamic and distributed over the large area. In this model, vehicles communicate with each other using uni-casting or multi-casting mode. In this model, each vehicle in the dynamic network has a neighbor list with location, unique-id, data, and credentials. The main objective of this model is to provide security and integrity to each vehicle in VANETs. Each vehicle is responsible to monitor its neighboring vehicles at the time of data communication process. Chaotic Hashing is an advanced cryptographic algorithm which is responsible for the conversion of variable-length binary string to fixed-length integrity value. Therefore, chaotic hash-based integrity verification techniques are more efficient and scalable than that of traditional hash algorithms in terms of resource usage and computational cost [10], [11]. In this proposed system, a novel chaotic hash model is used to generate a dynamic 1024, 2048, 4096-bit hash code as integrity value. In the VANET communication, each vehicle performs integrity verification and improved encryption on the communication data against malicious attacks.

Node Chaotic Integrity Algorithm

Input: M (Node data), Secret key, initialization parameters.

Step 1: Read VANET vehicle ID and Data D as M.

$$M = VehicleID(ID) + Data(D)$$

If message size is not multiple of 'n' then

Append the bit sequence 1000…000 at the end of the message.

Step 2: Divide the message into blocks of length n as

$B1, B2 \ldots\ldots Bm.$

Step 3: After padding, each block is again divided into' sub-blocks,

Each with 32-bit length and it is represented as $P_1, P_2 \ldots . P_m$.

Step 4: The Secret key is generated using the vehicle node's id and the chaotic uniform random function as.

$S = \text{Vehicle(id)} + \text{ChaoticUniformRN()}$

Where

Chaotic Uniform Random Number= $(2/\pi).tan^{-1}(\sqrt[3]{M})$

Generated secret key is initialized as X0 for the multi-chaotic system.

Step 5: An Extended multi-chaotic system with one of the dynamic chaotic map function

I.e. controlled Chebyshev Chaotic Map as:

Let n be a real integer x from the set G onto G such that,

$T_n(x) : G -> G : [-1,1] -> [-1,1]$

$T_n = k\cos(n.\cos^{-1} x)$ --(5)

The recurrence relation to the (5) is given as

$T_n(v) = (vT_{n-1}(v) - T_{n-2}(v)) / k$ -------(6)

and

$T_0(v) = k, T_1(v) = kv$ --------(7)

Step 6: In the transformation box, the following operations are performed

Initialize randomized permutation matrix as pkey.

Partition the byte array block into sub-blocks of 32 bits each.

For each sub-block
Do
M=PermutateMatrix();
M=pkey $M^{'} = (pkey^{T}.M) \bmod(1)$
N=pKey.kron($M^{'}$).scale(256);
Convert N into Hex string and append to NH.
Done

Step 8: Generates Hash value as

$$H_i = \text{Permute}(P^{'}_i)$$

$$\text{Hash } H = H_1 + H_2 + H_3 .... H_m$$

Generated hash H is used as the key for the proposed homomorphic encryption model.

This technique is effectively integrated with Bernoulli's mapping to enhance the overall randomness and performance.

Proposed Non-linear Double Encryption Model

Proposed encryption model has two phases to encrypt the VANET communication data. In the first phase, a polynomial based key generation process is performed using the non-linear curves generated using the dynamic chaotic maps. In the second phase, data is encrypted using the double encryption process. Iterative polynomial key generation phase

Choose two large random numbers m1 and m2 which are relative prime to multiplicative group $Z(n^2,*)$. Here $Z(n^2,*)$ is a multiplicative group with 'n' group order such that $o(n) \le o(Z(n^2,*))$.

In the proposed approach, a non-linear chaotic polynomial map is used to enhance the security parameters in the key generation process. The basic recursion relation for the non-linear equation is given as

$$T_n = kx + T_{n-2}$$

$$T_0 = 1$$

$$T_1 = k(1+\lambda^2)$$

Where λ is the randomized security parameter taken from $Z(n^2,*)$

Encryption Model - Key generation process for encryption model is initiated

Algorithm for key generation as shown in Figure 1.

Step 1: Select one of the polynomial equation with secret key s(k) as P(x)=s(k)*p(x)
Where p(x) is the curve taken from the family of curves. S(k) is the random element taken from group Z.

Step 2: Compute $\theta = \text{lcm}(g1-1, g2-1)$ and n=g1*g2. Where g1 and g2 are the elements taken from group Z.

Step 3: Select a number which is relative prime to θ as r1 and compute r2 as $r2 = \frac{\theta}{(r1+1)}$

Step 4: Select random parameters m1, m2, n1, and n2 from $Z(n,*)$

Step 5: Compute k1, k2, k3, k4 as

$$k1 = 1 + m2 * (g1 * g2)$$

$$k2 = k1^{m1} \bmod(n^2)$$

$$k3 = n1^{m1}.k1^{m1^2} \bmod(n^2)$$

$$k4 = n1^{m1}.n2^{r1.(g1*g2)} \bmod(n^2)$$

Step 6: Vehicle public key Pubk={k1,k2,k3,n1,g1.g2,P(x)}.

Step 7: Vehicle private key as Prik={m,r1,r2, θ ,s(k)}

Figure 1. Algorithm for key generation

Encryption Process

In encryption process, each vehicle's data is taken as input for data encryption using the double encryption process as shown in Figure 2. Decryption process as shown in Figure 3. Algorithm for encryption process as shown in Figure 4.

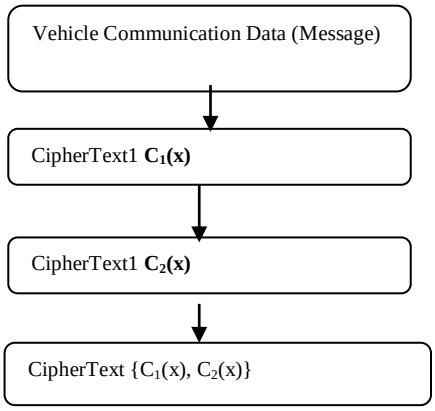

Figure 2. Double encryption process

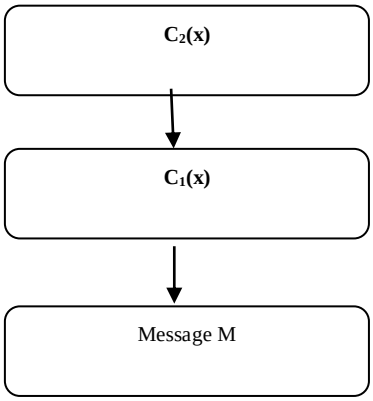

Figure 3. Decryption process

Input: Public key Pubk, Message M (byte array). Output: Ciphertext Procedure:
Convert message M into byte array as Bi
Compute Ciphertext 1: C1(x)
For each byte in Bi
Do
Convert Bi into binary string Bini.
Let l=|Bini|
PBini is the binary polynomial equation.
P(x) is the non-linear polynomial equation of degree n taken from the public key must satisfy
PBini=Py(x) mod s (k)
Where Py(x) is the equation in P(x).
Let Pd(x) is the equation in P(x) whose coefficients are powers of l.
Compute cipher text c1 as
C1(x) = Py(x) +s (k)* Pd(x)
Where C1(x) is the pre-encrypted message should satisfy the addition and multiplicative homomorphism.
Compute Ciphertext 2: C2(x). Select random factors f1, f2 and fb from Z (n,*).
Compute

$$\text{Let } B_i^{'} = C_1(x) \,//\, \text{ciphertext byte array}$$

$$CT_1 = k_1^{fb} \bmod (n^2)$$

$$CT_2 = k_2^{fb} \bmod (n^2)$$

$$CT_3 = n_1^{fb(f_1+1)} \bmod (n^2)$$

$$CT_4 = k_1^{fb}.f\ 2^{g1*g2} \bmod (n^2)$$

$$CT_5 = CT_1^{B_i^{'}}.CT_2.(k3)^{fb.f1} \bmod (n^2)$$

$$\text{Ciphertext } C_2(x) = \{CT_3, CT_4, CT_5\}$$

Figure 4. Algorithm for encryption process

Decryption Process

Decryption is the reverse process of the encryption process. Here, ciphertext2 is decrypted initially to find the ciphertext one and then the message will be decoded using the ciphertext one as shown in Figure 5.
Decoding C1(x):

Step 1: To decode C1(x) using cipher text C2(x), the following computation is performed using the keys as

$$Temp_1(\mathbf{x}) = \frac{F((CT_5 . CT_3^{r_1(g1*g2)-m_1})^{\frac{\theta}{(r1+1)}} \bmod(n^2)}{F(CT^{\theta}_4 \bmod(n^2))} \bmod(n)$$

$$C_1(x) = Temp_1(\mathbf{x}) - m_1 \bmod(n)$$

Where F is a decoding function defined by

$$F(x) = \frac{x-1}{g1.g2} \text{ for } x<n^2$$

Step 2: Decoding message using the $C_1(x)$ as

Message = $C_1(x) \bmod(s(k)) \bmod(2)$

Figure 5. Algorithm for decryption process

3. RESULTS AND ANALYSIS

Experimental results are designed and implemented using the java based VANET simulator and Real-time geographical map for VANET simulation. The basic properties of VANET simulator is given as shown in Table 2.

Table 2. Simulation Parameters

Parameter	Description
Simulator	VANET Simulator
Real-time Map	OpenStreetMap
Minimum number of Vehicles	50
Minimum number of Infrastructures	25
Communication data size	Variable
Minimum Memory required	4GB

3.1. Simulation Environment

Figure 6 describes the real-time traffic map for VANET simulation. This map is used to simulate the vehicles in the proposed model. Different paths and its outlines are shown in Figure 7. In Figure 8, communication of the vehicle is visualized with data security. During the data communication, each vehicle communicates with the other entities using the integrity verification method and the encryption method. Output of vehicle encrypted data as shown Figure 9.

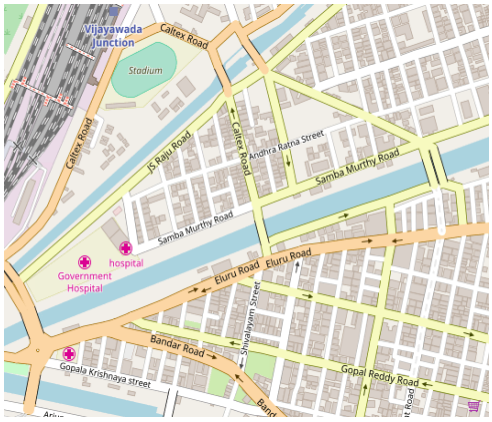

Figure 6. Input real-time vijayawada traffic map

Figure 7. Outline of map for VANET simulation

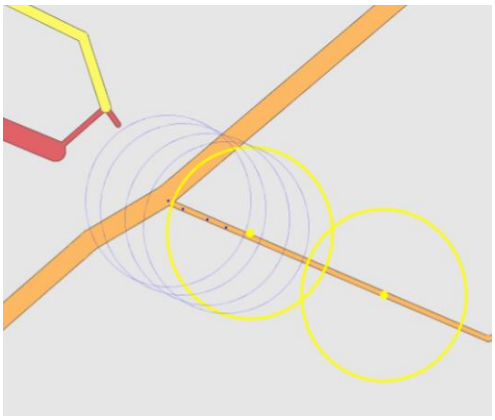

Figure 8. Vehicle communication along the given path

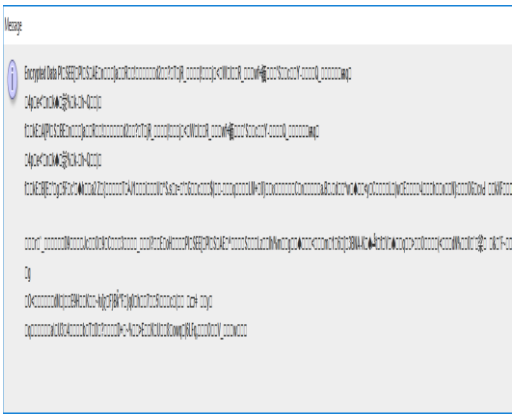

Figure 9. Output of vehicle encrypted data

Figure 10, illustrates the comparison of the proposed model to the existing models in term of a number `of vehicles to its communication runtime (ms). From the figure, it is clearly observed that the proposed model has less computational time compared to the existing models for security verification.

Figure 11 describes the performance of the proposed integrity value to the existing model for bit change in vehicle's hash value. Bit change defines the change in variation of hash binary value to the original binary value of the message. From the figure, it is clearly observed that the proposed model has high bit change variation compared to the existing models.

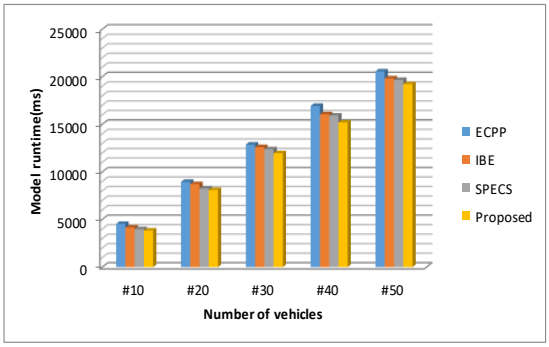

Figure 10. Comparision no of vehicles vs runtime

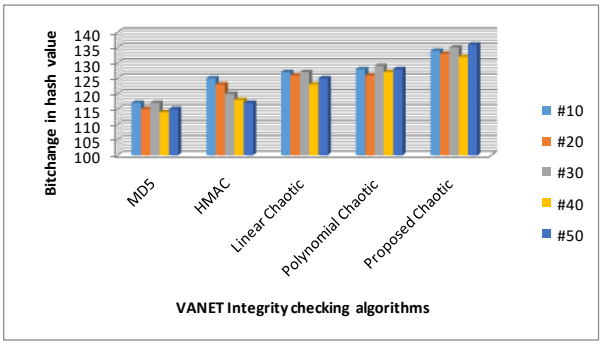

Figure 11. Proposed model interms of bit change

4. CONCLUSION

VANET is an effective and efficient approach which plays an important part role to improve traffic efficiency. To optimize the performance of the dynamic VANET networks along with trust, security, and authentication, a novel integrated framework for integrity verification is designed and implemented on real-time maps. Most of the traditional VANETs are vulnerable to data security, integrity and authentication due to change in dynamic topology. Also, Traditional security models require limited data size for data security between the V2V or V2I. In this paper, a novel vehicle integrity verification and encryption model is implemented on large geographical VANET map. The main objective of the proposed model is to improve the security of the V2V communication in large VANETs. In future, this work can be extended to large geographical routing map with an enhanced communication protocol in VANETs.

REFERENCES

[1] Papapanagiotou, K., Marias, G.F. and Georgiadis, P. (2007) 'A certificate validation protocol for vanets', IEEE Globecom Workshops, November, pp.1–9.
[2] J. Blum, A. Eskandarian, The threat of intelligent collisions, IT Prof. 6 (1) (2004) 24–29.

[3] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks," Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), Miami Beach, FL, 2007, pp. 257-267.
[4] A. Wasef and X. Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 78-89, Jan. 2013.
[5] R. Lu, X. Lin, H. Zhu, P. H. Ho and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, Phoenix, AZ, 2008.
[6] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing Public Key Infrastructure to Secure Vehicular Ad Hoc Networks", IEEE Wireless Communications, Vol. 17, No. 5, pp. 22-28, 2010.
[7] S. Jiang, X. Zhu and L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2193-2204, Aug. 2016.
[8] S. J. Horng et al., "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860-1875, Nov. 2013.doi: 10.1109/TIFS.2013.2277471
[9] Deng SJ, Li YT, Xiao D (2009) Analysis and improvement of a chaos-based hash function construction. Commun Nonlinear Sci Numer Simulat 15:1338–1347.
[10] Akhavan A, Samsudin A, Akhshani A (2009) Hash function based on piecewise nonlinear chaotic map. Chaos Solitons Fractals 42:1046–1053.
[11] Xiao D, Peng WB, Liao XF et al (2010) Collision analysis of one kind of chaos-based hash function. Phys Lett A 374:1228–1231.
[12] Li Y, Xiao D, Deng S, Han Q, Zhou G (2011) Parallel hash function construction based on chaotic maps with changeable parameters. Neural Comput Appl 20(8):1305–1312.