Design of High Secured Multi Scroll Attractor Based Henon Map Chaotic Encryption Scheme for VANET Communication

DOI : 10.36909/jer.ICETET.14973

G Bindu [1], Dr. R .A Karthika [2],

Department of Computer Science Engineering, Vels Institute of Science Technology and Advanced Studies (VISTAS),

E-mail : bindu.se@velsuniv.ac.in; Corresponding Author.

ABSTRACT

The vehicular ad hoc networks are vulnerable to security threats while communication is established in wireless made proper encryption scheme can aid in establishing effective and secure communication. Conventionally group key agreement model (GKA) scheme is widely used for enabling security in VANET networks which is insignificant because of their over exploitation of resources in the network. In order to establish a secure communication in VANETs, a novel multi scroll attractor (MSA)based chaotic Henon maps encryption approach is proposed. The extensive experimentations has been carried out in the proposed scheme and it proves to satisfy all the security requirements of VANET scenario.

Keywords: VANET, Chaotic system, encryption, Henon Maps.

INTRODUCTION

VANET models are attractive on demand communication schemes in on-road traffic management systems [1-3]. This tremendous growth of IoT and 5G communication schemes make VANET more efficient in developing automated traffic flow control system. The major spots of VANET includes the roadside Unit (RSU), vehicle and the On Board Unit (OBU) to establish a link. The link established connecting the three units RSU, vehicle and OBU keeps on communicating the vehicle speed, vehicle ID, driver status, direction change status and other road related information.

This communication should be true enough such that the receiving end takes decision regarding the messages received. If suppose the message received is wrong, the traffic collision occurs often leading to accidents. Thus genuine timely communication is the most needed part in developing a good VANET model. The communication must be secure enough, so that the traffic flow will be smooth. As like other communication links, VANET communication is also highly susceptible to instruction and cyber-attacks. If the message get miscommunicated, entire VANET system will collapse. Thus encryption of messages are highly demanded in an efficient VANET design.

The security schemes deployed in traditional VANET's are inefficient and high resource utilizing schemes. The encryption scheme must ensure proper security, privacy concerns and should uphold the efficiency of the VANET. Ensuring secure communication is most vital requirement for any VANET system [4]. VANET enables the system to replicate dynamic behavior. The switching and connection between nodes keeps on changing dynamically makes the system more vulnerable to attacks. In traditional encryption schemes, a common key is generated and used to secure the communication with in a link.

The group key agreement method [5-8] is a key based encryption scheme which helps in transmitting messages among the links. The increased number of nodes in the network further increase the challenge in key generation and it makes the schematic inefficient. But in real time scenarios, the multi path communication creates more instability in sharing a common secret key to more number of nodes in the dynamic VANET system. The authenticity of information is the major goal in deploying efficient encryption schemes. This paves the path for a complete session key generation once the communication is established to secure the system.

The dynamic nature of VANET can easily suits with the chaotic encryption schemes due to the flexibility in network. Chaos based encryption gains promising outcomes in session key generation recent times. Construction of chaotic encryption model is challenging due to the need for structural design changes based on the application they are deployed. The randomness in chaotic systems are preferred for VANET models [8-11].

RELATED WORKS

Huang et al (2011) introduced a batch authenticated and key agreement model (ABAKA) to secure more than one transmission at the same time. In crowded traffic system, this model finds to be helpful for encryption of information. Also the scheme reduces the overall delay in decrypting back the data and overall transmission time is conserved. Mohammad Wazid et al (2019) designed and developed an authenticated key management (AKM) scheme which implies with fog based prediction scheme. The AKM scheme helps establishing secure communication in VANETs and are validated with the AVISPA tool. Fog based computing scheme is a derived form of mobile cloud computing domain. Prabhjot Singh et al (2018) proposed a secure network system for VANET models. An elliptical curve shaped cryptographic scheme is deployed to secure the information in the VANET links. Amit Dua et al (2017) proposed a queuing based algorithm based on game theory approach to secure the communication links. The algorithm controls the resource parameters such as bandwidth, distance and fidelity of entire network. Rasmeet S Bali et al (2015) developed a clustering based security approach for VANET systems. This grouping of nodes and key generation is effective in collision free networks. Nikolaos Alexiou et al (2013) evolved with an idea of generating tokens for cryptography to develop privacy in individual links. This helps in authenticity of information in VANETS. Majid Mobini et al (2017) developed a hybrid model that involves an OFDM combined chaotic encryption. This aids in generating cipher text for the original message before transmission. At the receiving end the cipher text is decrypted to retrieve the original message. The drawback is it the proposed model is time constraint and also the complexity is leveraged to fit for VANET which will not be helpful in practical deployment. Prabakeran et al (2020) developed a chaotic system based on dragonfly swarm optimization to optimize the data in the RSU. The RSU based encryption is mainly deployed to access the misbehaving nodes in the network and to learn about the intruding attacks in RSU.

From the literature, it is evident that most conventional key generation based encryption schemes are resource consuming and are vulnerable to strong attacks in various node levels. The chaotic cryptographic schemes deployed so far is made at the RSU end which is less efficient. Thus the proposed MSA-chaotic Henon maps model is developed to perform encryption in the On Board Unit (OBT).

SECTION-III

PROPOSED ARCHITECTURE

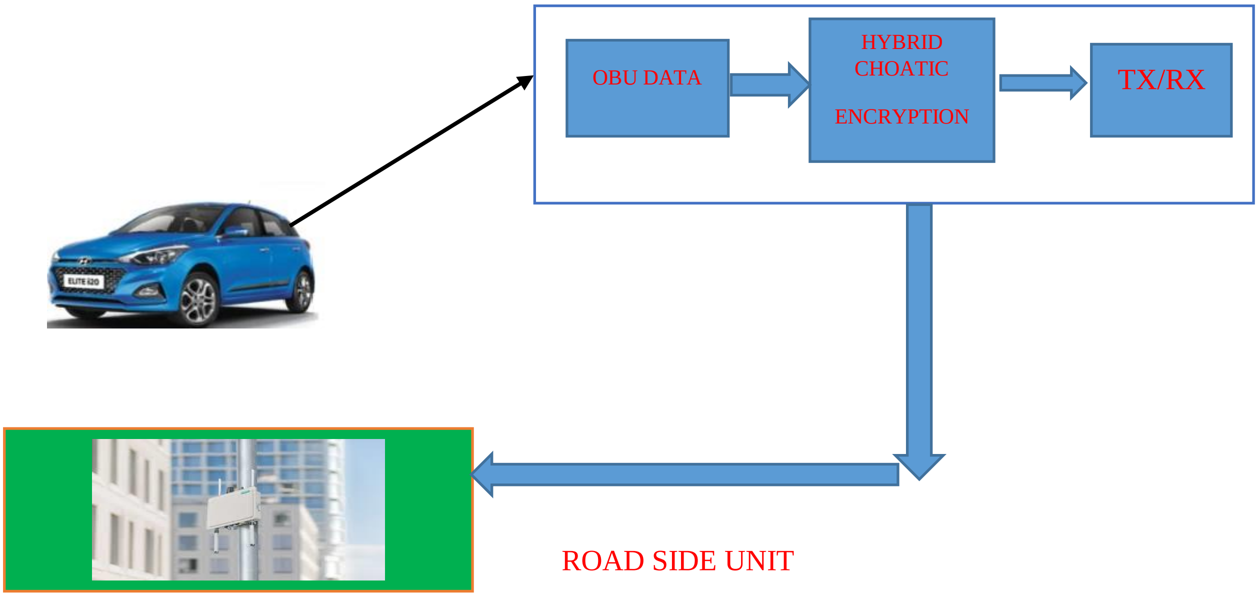


Figure 1 Proposed Security Framework For the Vehicular Networks

SYSTEM OVERVIEW

The proposed security encryption methodology for the VANET system. The proposed model works on the hybrid combination of Multi -scroll Henon Attractors (MSHA) and used to transmit the on-board unit (OBU) data to the Road Side Unit (RSU). The engine diagnostic data, vehicle’s and authenticator‘s information data were taken as the inputs for authentication. The working mechanism of each and every module has been discussed in the preceding section.

PROPOSED ENCRYPTION MODELS:

MULTI-SCROLL ATTRACTORS

The dynamic properties of multi scroll attractors are interesting for complex applications than most of the chaotic systems. Chaotic systems usually exhibit their existence of third state in a dynamic model which can be expressed as

$\dot{x} = -px + qyz$ (1)

$\dot{y} = -ry3 + sdz$ (2)

$z = tz - fxy \dot{+} O1 \tanh(y + g)$ (3)

The initial conditions are set arbitrarily as 0.1, 0.1 and 0.6. From Eqn (1), $p, q, r, s, t, f, O1$ and g are the chaotic parameters which constitudes corresponding values as 2,6,6,3,3,1,1 and 2. The term g is a varying function that can generate multiple scrolls. The encryption of chaotic systems are complex in nature.

When the hyperbolic function is introduced in first state with the parameter $g = -3$and for the initial conditions$[0.1, -0.1, -0.6]$ it shows double scroll attractor which is shown in Figure 1.When introduced in the second state, with parameters$p_1 = -1$, $g = 3$and initial conditions $[0.1, -0.1, -0.6]$ it shows four scroll which is shown in Figure 2. While in the third state with parameters$p_1 = 1$, $g = 3$and initial conditions [0.1,0.1,0.6] it shows single scroll which is shown in Figure 3. Thus we can confirm that the system holds multiscroll property.

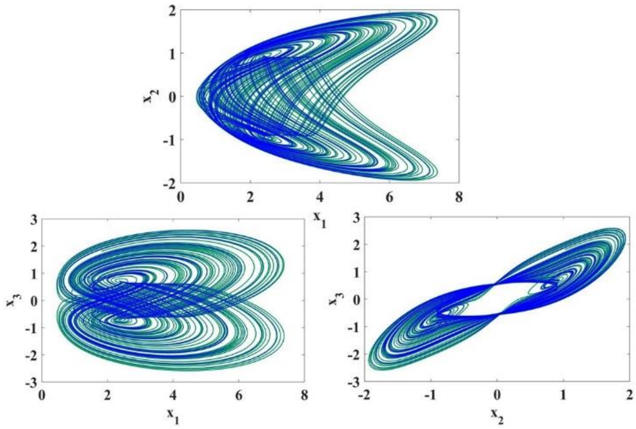


Figure 2. Phase portraits of cubic nonlinear system with $p_1\, tanh(\, x_2 + g)$ function in 1st state

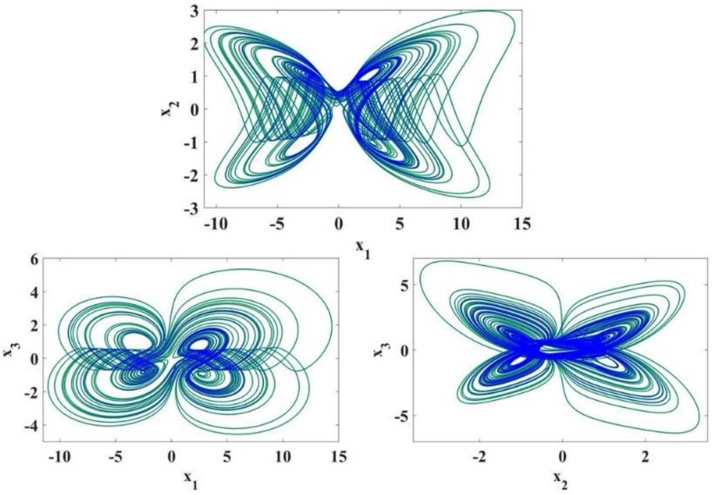


Figure 3. Phase portraits of cubic nonlinear system with $p_1\, tanh(\, x_2 + g)$ function in 2nd state

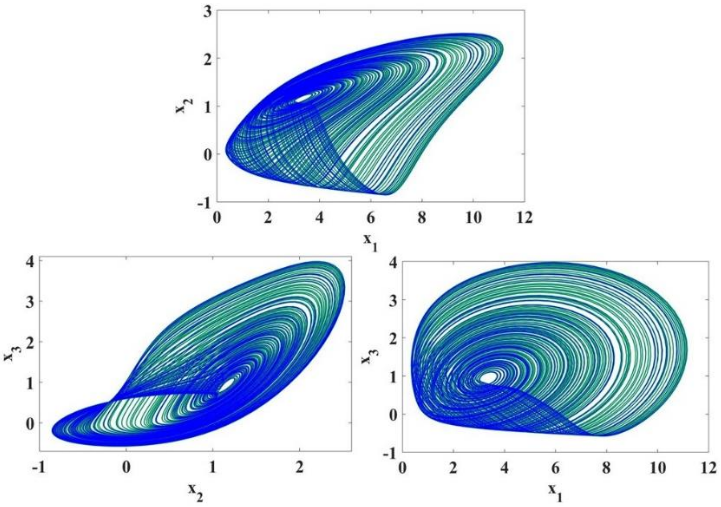


Figure 4. Phase portraits of cubic nonlinear system with $p_1\, tanh(\, x_2 + g)$ function in 3rd state

The bifurcation characteristics of multi- scroll attractors are given in the following figures 5.

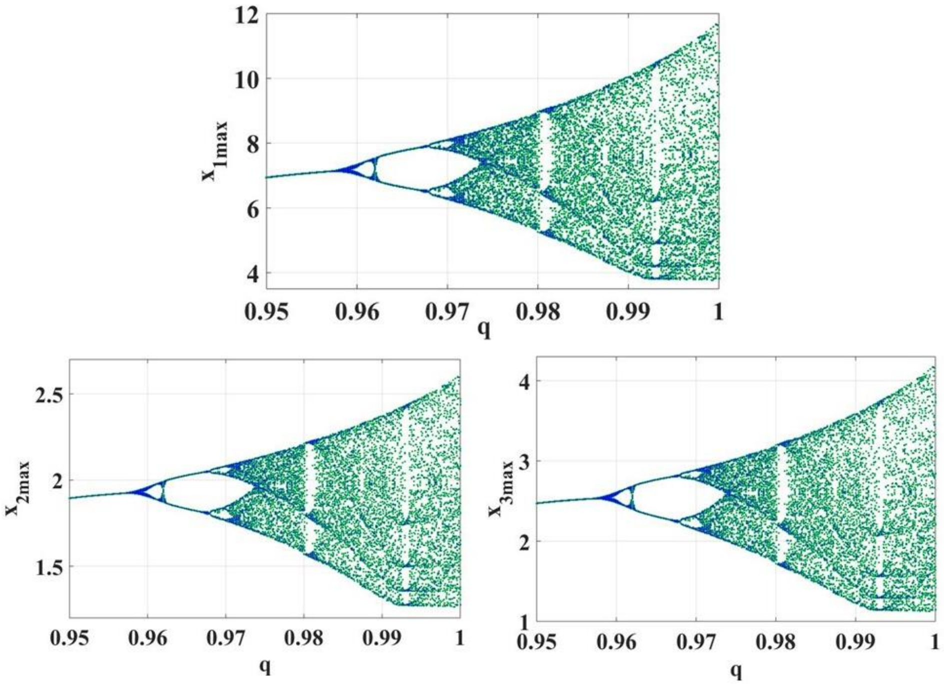


Fig 5 Fractional Bifurcation Diagrams for the Proposed Multi Scroll Chaotic Systems

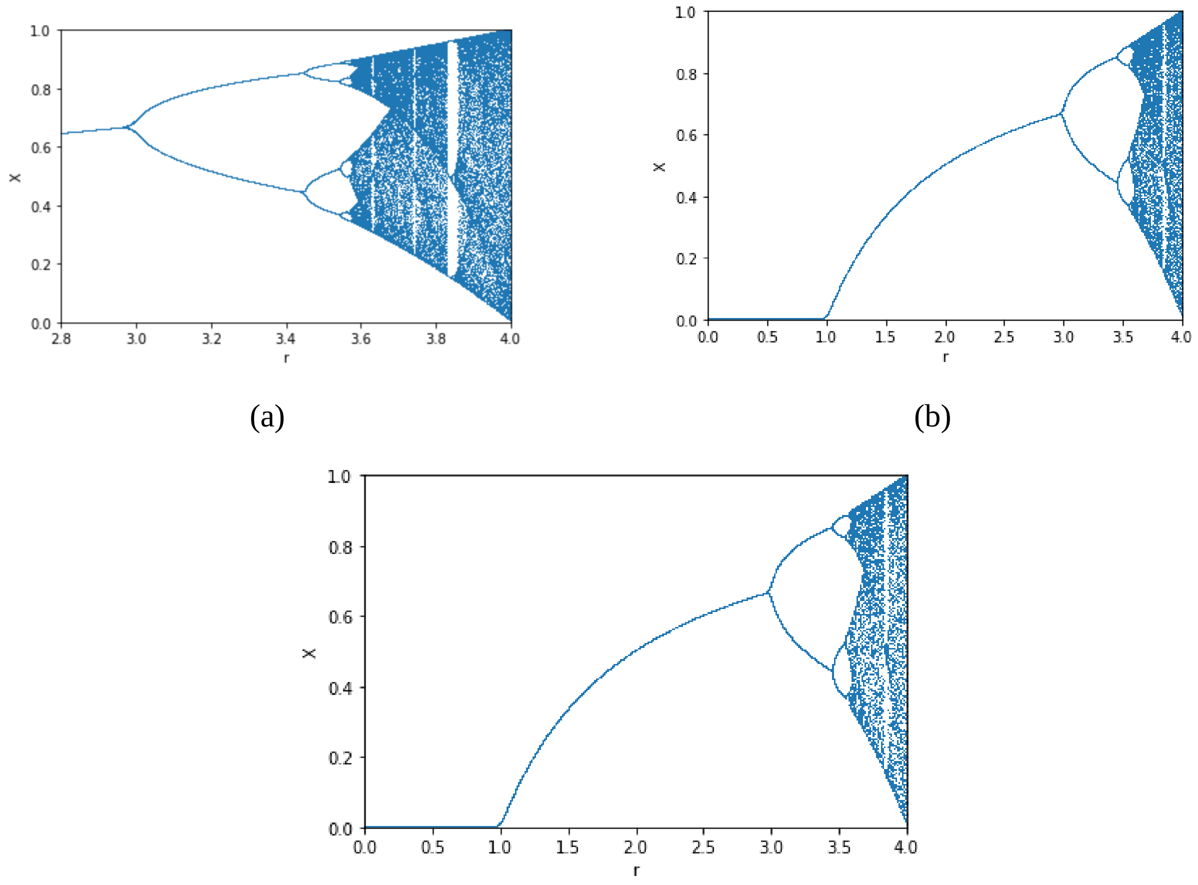
HENON MAPS

In earlier 70’s Henon proposed a 2-D invertible chaotic system. The mathematical expression of Henon map is given by

$$x_{(n+1)} = 1 - ax_n^2 + y_n \tag{4}$$

$$y_{(n+1)} = bx_n \tag{5}$$

The terms a, b constitutes the bifurcation parameters. The contraction factors in the 2-D Henon map is independent of x and y. From multiple trials, the bifurcation parameters are set as a = 1.4 and b = 0.3 to establish a chaotic nature. The two bifurcation function generates bi-periodic oscillations exhibiting doubling oscillation behavior. The value of a ranges from 0.85 to 1.1 for double periodic oscillation occurs. The bifurcation characteristics of Henon maps are given as follows (Fig 6)



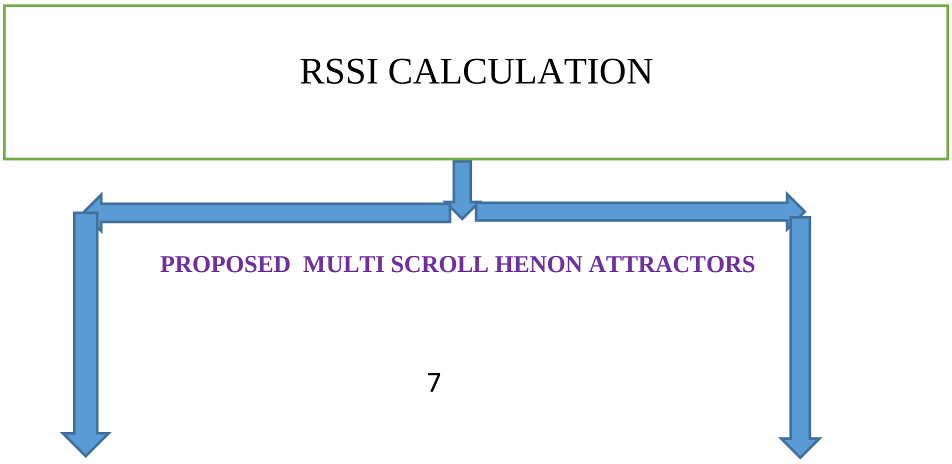
(a)

(b)

©

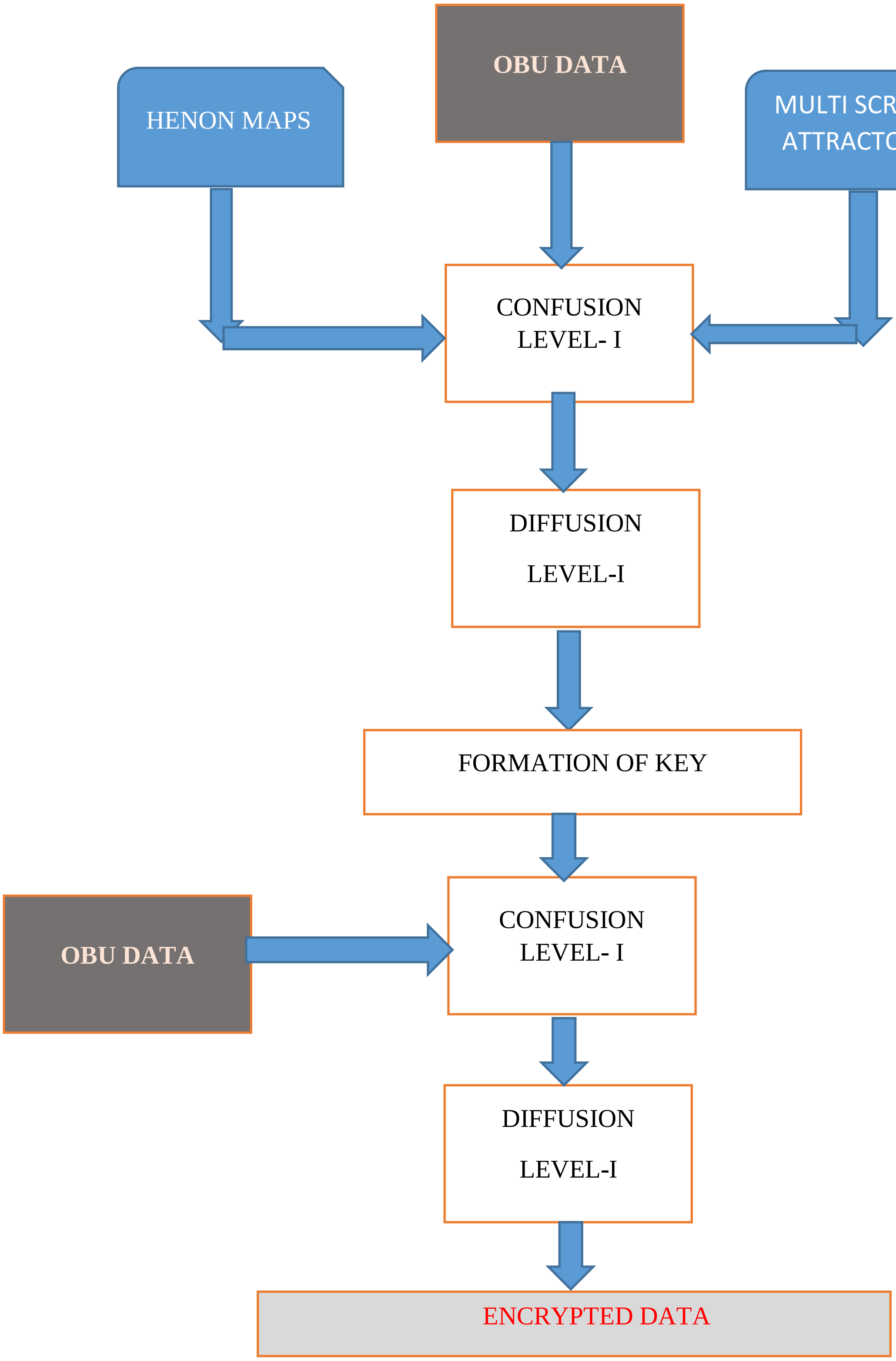
Figure 6 Bifurcation Characteristics of Henon Maps at Different Initial Conditions

PROPOSED ENCRYPTION MODEL



RSSI CALCULATION

PROPOSED MULTI SCROLL HENON ATTRACTORS



GENERATION OF INITIAL CONDITIONS

As discussed in the previous section 3.2, role of initial condition increases the sensitivity of the chaotic systems. In order to ensure more randomness in the data, this research proposes the measurement of received signal strength (RSS) of the wireless transceivers used on the on-board units(OBU) .Since the RSS exhibits dynamic nature in accordance to the distance, usage of RSS in the proposed model has proved to be more random and the mathematical expression of RSS determination is given by

$$\textbf{RSSI}=\mathrm{Pt}-\mathrm{PL(D)}. \qquad (6)$$

$$D = 10\left[\frac{(P_o - F_m - P_r - 10n\,log(f) + 30n - 32.44)}{10n}\right] \qquad (7)$$

Where P_o is the power of the signal (dBm) in the zero distance,Pt is the transmitted power, Pl=Power Loss at distance, $P_r$is the Signal power (dBm) in the distance d, $f$is the signal frequency in MHz, $F_m$is the Fade margin and n is the path-loss exponent.

MULTI-SCROLL HENON ATTRACTORS

The propose chaotic maps consist of the combination of the both multi scroll attractors and henon maps. The characteristics behavior of the proposed chaotic systems with the RSS as initial conditions are shown in Figure .The complete encryption process involved using the proposed chaotic maps are detailed as follows

Step 1: Measure the RSSI (Received Signal Strength Indicator) using the mathematical expression (6) and (7)

Step 2: Form the RSSI based henon Maps which are then formulated as matrix G

Step 3: Form the RSSI based Multi Scroll Attractors which is represented by matrix H

Step 4: Pseudo Random Matrix is formulated by performing the XOR operation between the G and H matrix and stored as' J' matrix with the mathematical formula

$$J = (\ |G|\ \hat{}\,|H|\ )\ \mathrm{mod}\ 256 \qquad (8)$$

Step 5: The 'n' number of OBU data is then confused (permutation) and diffused with the J matrix to form the key matrix'T'

$$T = \{\ |n|\ \Theta\ |J|\}\ \mathrm{Mod}\ 256 \qquad (9)$$

Step 6: Again the encrypted data (cipher data) is formed by the two tier operations of permutation and diffusion with the T matrix

$$Y = \ \{\ |n|\ \Theta\ |T|\}\ \mathrm{Mod}\ 256 \qquad (10)$$

SECTION-IV

RESULTS AND DISCUSSION

SIMULATION PARAMETERS

The extensive testing of the proposed MSA-chaotic Henon map scheme is implemented using SUMO-OMNET tool and the analysis is performed using Python 3.7. The simulation parameters are tabulated as follows.

Table 1. Simulation Parameters for the proposed MAHM model

Sl.no	Specifications	Parameters Used
01	No of Vehicles	50
02	Source of Data	OBU-On board Units
03	Receiver	RSU- Road Side Unit
04	No of data transmitted	100 bytes
05	Speed of the vehicles	20-40 Km/hr
06	Communication Mode	WAVE framework/IPv6

STATISTICAL RANDOMNESS ANALYSIS

The security is well established in network based on the weightage of key generation mechanism and respective encryption and decryption procedures. Usually the encryption schemes employed in dynamic systems exhibit symmetric property which adds vulnerability for multiple attacks. Thus randomness in key generation is the ultimate purpose of encryption schemes.

The pseudo random generator in cryptographic application are more important due to unpredictable reasons. A set of statistical tests for the randomness of number sequences is labeled by The National Institute of Standards and Technology (NIST) to confirm that the assumed random or Pseudo-Random generator can be used for cryptographic applications. The randomness attained at each stage has to be registered with arbitrary values. In the testing phase, the NIST test set is iterated and converted in to binary variables validated in python libraries implemented in embedded boards.

FREQUENCY MONOBIT TEST

The test focuses in detection of zeros and ones for binary sequence. The test determines the availability of ones and zeros in the sequence to be a true data. The test value calculates the nearness of the fraction of ones to ½, that is, the quantity of ones and zeroes in a sequence should be about the same. All subsequent tests be influenced by the passing of this test. In this test, zeros are assigned with -1 and ones are assigned with +1 and added to yield the cumulative numbers whose overall mathematical expression is given as follows as

$$S = ||S(n)||/n^{0.5} \qquad (11)$$

Where S (n) is the sum of the values obtained and n is the total samples. Once the sum of values are calculated, the randomness function is expressed as P value given by

$$P= \mathrm{erfc}(S/(2)^{\wedge}0.5 \qquad (12)$$

No of iteration	Test nature	Decision Rule	Randomness value	Key Test
1	Frequency Monobit	P>0.01	P=0.0778900	PASS
2			P=0.0664323	
3			P= 0.0565443	
4			P=0.0565721	
5			P=0.046896	
6			P=0.026789	
7			P=0.0332467	
8			P=0.0643210	
9			P=0.07646262	
10			P=0.0567171	

The parameters attained through the frequency monobit tests are tabulated. In the consecutive ten cycles, the key generated by the chaotic Henon maps represented the existence of randomness with compatibility for encryption purposes to withstand major threats.

FREQUENCY BLOCK BIT

The aim of frequency test is to find the availability rate of ones in a k-bit block. The frequency of occurrence of ones in a single k-block is expected to be half of the block size. In this frequency test, K -bit encryption is sub-divided into the K/2 for every iteration whose randomness is calculated by the mathematical expression

$$P = igamc(\frac{N}{2},\frac{\yen^{0.5}(obs)}{2}) \tag{13}$$

Where $igamc$ is the gamma function for estimation of randomness.

No of iteration	Test nature	Decision Rule	Randomness value	Key Test
1	Frequency Block bit	P>0.01	P=0.0202920	PASS
2			P=.0363425	
3			P= 0.045262	
4			P=0.063002	
5			P=0.034210	
6			P=0.0234562	
7			P=0.043512	
8			P=0.010192	
9			P=0.028999	
10			P=0.0452672	

For every cycle of process, the P value greater than 0.01 is exemplary and the key is tested under this condition.

RUN TEST

The aim of the run test is to analysis the available runs in one complete sequence till the run is interrupted by non-identical bit sequence. The run length of k will have same bits until a non-identical occurrence is observed. The number of occurrence of ones and zeros of continuous length are observed with such test. It also relates the oscillation of zeros and ones in a single sequence. The key's endurance is looked at for its randomness is expressed as

$$P = erfc(|V(n)(obs) - 2n\pi(1-\pi)|)/2.828n\pi(1-\pi) \tag{14}$$

Where V (n) (obs) = has to be done

No of iteration	Test nature	Decision Rule	Randomness value	Key Test
1	Run test	P>0.01	P=0.011278	PASS
2			P=0.067829	
3			P= 0.012909	
4			P=0.03561	
5			P=0.02356	
6			P=0.01890	
7			P=0.012010	
8			P=0.0290783	
9			P=0.010101	
10			P=0.019022	

In this test, V(n)(Obs) exhibited the faster oscillations (Oscillations is considered as the switch from one to zeros).Hence the profound randomness attained are created by the proposed MSACHM model.

LONGEST RUN TEST

The test of longest identical run test is performed to detect complete one runs in M-bit sequence. This shows the occurrence of consistent ones in attest sequence. The irregularity noticed by the model is tested with different M-values applied with NIST standard is tabulated as follows.

Minimum n sequence	Maximum M values
128	8
6272	128
750,000	10^4

The randomness value P is expressed mathematically as in Eqn (14).

Iteration	N	N1	N2	D1	P	Key test(P>0.1)
1	256	42	67.3	-1.456298	0.044536	
2	256	43	65.5	-3.6789	0.089522	
3	256	28	76.0	-6.8920	0.067890	
4	256	31	54.0	-1.83536	0.047425	

5	256	30	78.0	-4.890	0.052101	PASS
6	256	31	65	-2.7242	0.029202	
7	256	22	66	-2.6412	0.034910	
8	256	57	68	-3.8902	0.05234	
9	256	78	69	-4.6782	0.09876	
10	256	45	65	-1.9087	0.012892	

DFT TEST

The Discrete Fourier Transform (DFT) based test are conducted to calculate the maximum peak value in a sequence. This shows the existence of deviation from the hypothesis of randomness. The purpose is to detect whether the number of crests exceeding the 95 % threshold is considerably different than 5 %. The mathematical expressions are derived as follows.

Iteration	N	N1	N2	D1	P	Key test(P>0.1)
1	256	38	67.3	-2.456298	0.056472	
2	256		65.5	-4.5890	0.09876	
3	256	45.3	76.0	-7.46789	0.078362	
4	256	45	54.0	-1.8930	0.045678	
5	256	47.2	78.0	-4.5789	0.053637	PASS
6	256	54	65	-2.5700	0.01789	
7	256	43	66	-2.7650	0.025678	
8	256	57	68	-3.8902	0.05234	
9	256	58	69	-4.6782	0.09876	
10	256	43	65	-1.9087	0.012892	

Thus the important condition for randomness confirmation should be less for d and P should be greater than 0.01.

KEY SENSITIVITY

The sensitivity of the dynamic systems are profound for the analysis of Pseudo randomness in chaotic systems. This metric ensures secure encryption of data that are communicated between the devices.

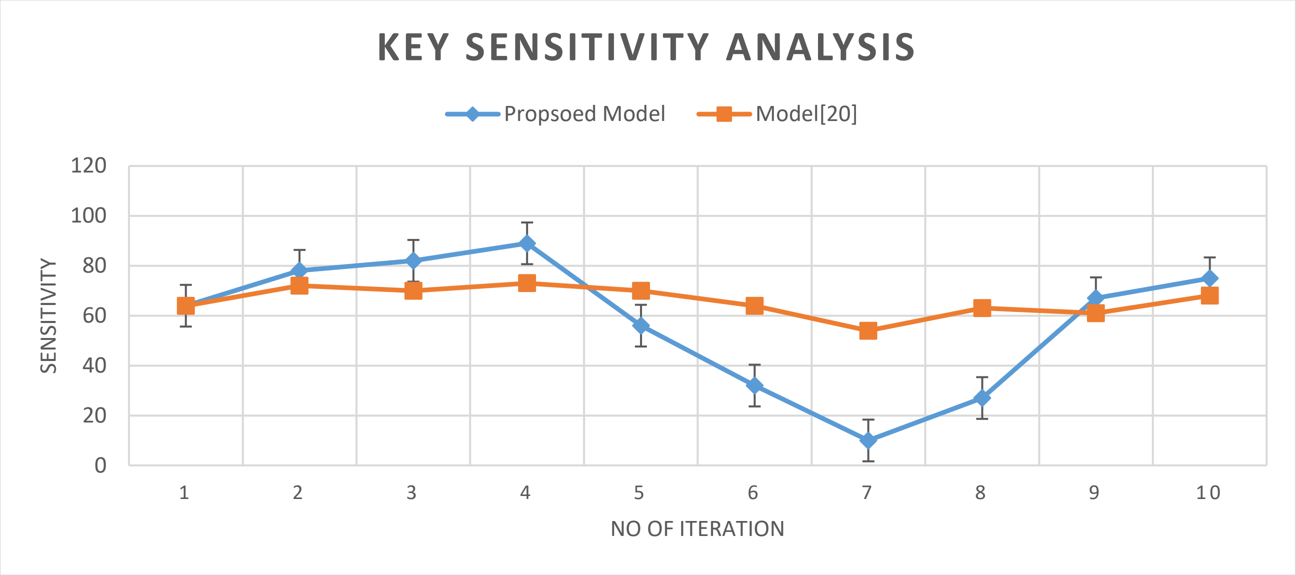


Figure 7 Key Sensitivity Analysis between the Proposed Model and the Model proposed by Jie Chu etal.

Figure7 shows the comparative analysis between the proposed algorithms and other existing model mechanism. The single chaotic algorithm exhibits the good randomness but the randomness in high for the proposed MSA- chaotic Henon map model when compared with single chaotic applications.

SECTION-V

CONCLUSION

As discussed in the article, the chaotic behavior of data transmission in VANET are more prone to cyber threats. Proper encryption schemes should be deployed to overcome such threats. Conventional key generation schemes are vulnerable to attacks due to the dynamic nature of the network. Chaotic encryption schemes use random key generation for encryption. The proposed MSA-Chaotic Henon Map encryption model helps in highly sensible pseudo random code generation for data transmission in VANET. The effectiveness and order of encryption scheme has been studied and finds valid for VANET systems.

REFERENCES

[1]Al-Fuqaha, A., Gharaibeh, A., Mohammed, I., et al.: ‘Online algorithm for opportunistic handling of received packets in vehicular networks’, IEEE Trans. Intell. Transp. Syst., 2018, PP, (99), pp. 1–12

[2] Yan, G., Olariu, S.: ‘A probabilistic analysis of link duration in vehicular ad hoc networks’, IEEE Trans. Intell. Transp. Syst., 2011, 12, (4), pp. 1227–1236

[3] Chang, C.J., Cheng, R.G., Shih, H.T., et al.: ‘Maximum freedom last scheduling algorithm for downlinks of DSRC networks’, IEEE Trans. Intell. Transp. Syst., 2007, 8, (2), pp. 223–232

[4] Oh, H., Yae, C., Ahn, D., et al.: ‘5.8 GHz DSRC packet communication system for its services’. IEEE VTS 50th Vehicular Technology Conf., Amsterdam, Netherlands, 1999, 4, pp. 2223–2227

[5] Liu, L., Wang, J., Huang, J., et al.: ‘Encounter prediction-based data forwarding for high reliability in bus networks’, Ad Hoc Sens. Wirel. Netw., 2018, 41, (1–2), pp. 137–164

[6] Dahiya, P.K., Singh, V.: ‘Security issues in VANETs’. TEQIP Sponsored National Conf. Technical Collaboration with IEEE-EMBS/IMS Delhi chapter, Anaheim, USA, 2010

[7] Emara, K., Woerndl, W., Schlichter, J.: ‘Poster: context-adaptive user-centric privacy scheme for VANET’. Int. Conf. Security and Privacy in Communication Systems, Dallas, USA, 2015, pp. 590–593

[8] Cui, J., Zhang, J., Zhong, H., et al.: ‘SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter’, IEEE Trans. Veh. Technol., 2017, PP, (99), p. 1

[9] Jiang, Y., Ji, Y., Liu, T.: ‘An anonymous communication scheme based on ring signature in VANETs’, abs/1410.1639, pp. 1–20 [10] Chen, H., Li, W., Su, Y.: ‘Certificate-based proxy ring signature scheme’, Comput. Eng., 2012, 38, (16), pp. 149–152

[11] Zeng, S., Huang, Y., Liu, X.: ‘Privacy-preserving communication for VANETs with conditionally anonymous ring signature’, Int. J. Netw. Secur., 2015, 17, (2), pp. 135–141

[12] Lang, W., Yang, Z., Cheng, W., et al.: ‘A new improved ID-based proxy ring signature scheme from bilinear pairings’, J. Harbin Inst. Technol. (New Series), 2006, 13, (6), pp. 688–691 .

[13] Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An efficient identitybased batch verification scheme for vehicular sensor networks,” in Proc. of the 27th Int. Conf. on Computer Communications-IEEE INFOCOM 2008. Phoenix, AZ, USA: IEEE, 13-18 April 2008, pp. 816–824.

[14] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, “RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks,” in Proc. of IEEE Int. Conf. on Communications (ICC 2008). Beijing, China: IEEE, 30 May 2008, pp. 1451–1457.

[15] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. of 4th Annual Int. Cryptology Conf. on Advances in CryptologyCRYPTO 1984. Santa Barbara, CA, USA: Springer-Verlag, Berlin, 19-22 August 1985, pp. 47–53.

[11] Y. Liu, L. Wang, and H.-H. Chen, “Message authentication using proxy vehicles in vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 64, no. 8, pp. 3697–3710, 2015.

[12] Xiaoliang Wang, Shuifan Li, Shujing Zhao & Zhihua Xia (2017) A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm, Automatika, 58:3, 287-29412

[13] Maryam Rajabzadeh Asaar∗, Mahmoud Salmasizadeh, Willy Susilo. A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks. IEEE Transaction on Vehicular Technology.

[14] Mohammed GH. Al Zamil , Samer Samarah , Majdi Rawashdeh, M. Shamim Hossain. False-Alarm Detection in the Fog-Based Internet of Connected Vehicles. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 68, NO. 7, JULY 2019

[15] Samuel Kofi Erskine, Khaled M. Elleithy. Secure Intelligent Vehicular Network Using Fog Computing. Electronics 2019, 8, 455; doi:10.3390/electronics8040455

[16] D. Manivannana, Shafika Showkat Monia, Sherali Zeadall. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)

[17] P. Asuquo, H. Cruickshank, J. Morley, C.P.A. Ogah, A. Lei, W. Hathal, S. Bao, Z. Sun, Security and privacy in location-based services for vehicular and mo-bile communications: an overview, challenges and countermeasures, IEEE Int. Things J. (Early Access) XX (2018)

[18] K. Taimur, A. Naveed, C. Yue, S.A. Jalal, A. Muhammad, S. ul Haq, C. Haitham, Certificate revocation in vehicular ad hoc networks techniques and protocols: a survey, Sci. China Inf. Sci. 60(10) (2017).

[19] Krauss, S., Microscopic modeling of traffic flow: Investigation of collision free vehicle dynamics, 1998

[20]. Wagner, P. and Lubashevsky