A Design of Highly-Secured Map Chaotic Encryption Scheme for VANET Communication

Christalin Nelson S[1,2*], Ram Karan Singh[1], G.L.Prakash[3]

1 ITS, ICFAI University, Dehradun., Uttarakhand, India.
[2] School of Computer Science, Univ. of Petroleum & Energy Studies, Bidholi, Dehradun, India.
[3] Dept. of Information Science & Engineering, BMS Institute of Technology, Karnataka, India.
christalinnelson@gmail.com

Abstract. In the realm of wireless communication, Vehicular Ad Hoc Networks (VANETs) confront security vulnerabilities, necessitating the adoption of an encryption method that ensures efficient and secure communication. VANETs typically rely on the group key agreement model for security, but this approach proves ineffective due to resource overuse within the network. To establish secure communication in VANETs, this study proposes an innovative, lightweight, and robust protocol that utilizes Network-Centric Henon-Logistic-Chaotic Maps (NC-HLM) to ensure a high level of security among vehicles. The suggested methodology enables legitimate vehicular devices to periodically update their keys during each gearbox iteration and privately transmit the dynamically generated key authentication for secure data transmission from source to destination. Formal analysis using the Burrows-Abadi-Needham Logic (BAN) was conducted to assess and evaluate the security strength of the proposed model, and comprehensive validation was carried out using NIST (National Institute of Science and Technology). The results unequivocally demonstrate that the proposed system exhibits robust security characteristics against both active and passive attacks. Furthermore, this approach effectively addresses the limitations of current security techniques and significantly outperforms existing designs.

Keywords: VANET, Chaotic System, Henon Logistic Chaotic Maps, Group Key Agreement, Encryption, NIST, BAN.

1 Introduction

VANETs serve as advanced on-demand communication systems for efficiently managing road traffic flow in response to the rapid expansion of IoT and 5G communication technologies [1]. VANETs rely on key components such as the roadside unit (RSU), vehicles, and onboard units (OBUs) to establish connections that transmit critical vehicle information, including speed and ID, to ensure seamless traffic flow control. For this communication to be effective, it must be highly accurate and secure, as VANETs are susceptible to various security threats, similar to other communication channels. Therefore, any well-designed VANET system must prioritize message encryption to prevent miscommunication [2].

© The Author(s) 2023
C. Kiran Mai et al. (eds.), *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)*, Atlantis Highlights in Computer Sciences 18,
https://doi.org/10.2991/978-94-6463-314-6_19

Traditional VANET security methods are ineffective and resource-heavy. Ensuring VANET efficiency, robust security, and privacy is essential [3, 4]. VANETs' dynamic nature makes them vulnerable, to changing nodes and connections. Encryption relies on shared keys from conventional algorithms. Group key agreement aids message transmission [5-8], but as nodes grow, key challenges arise, reducing effectiveness. Sharing a common key with multiple nodes in a dynamic setup introduces instability. Effective encryption ensures data integrity and full-session key protection post-communication establishment.

The adaptability of VANET's dynamic nature makes it conducive to integrating chaotic encryption algorithms. However, developing chaotic encryption models tailored to specific applications within the VANET framework is challenging due to the network's structural modifications. VANET models benefit from the unpredictability characteristic of chaotic systems [9, 10]. This research utilizes hybrid Henon-logistic maps, inspired by the chaos encryption concept, to secure sensitive data from vehicles.

This paper introduces a novel lightweight encryption technique that leverages the hybrid concept of network-centric Henon-Logistic maps. The initial conditions of these maps are optimized based on network parameters to achieve a high degree of randomness and robust security. Furthermore, the suggested protocol uses NIST tests to confirm its randomness and its ability to withstand attacks. Comparative analysis with existing schemes demonstrates that the proposed approach is superior, effective, and highly secure against attacks, fulfilling the objective of a secure design.

2 Related Works

Manimekala et al. conducted an analysis of security concerns and challenges in VANETs. Their work not only categorized various VANET usage scenarios but also addressed security risks, prerequisites, and proposed topologies to enhance security. They also discussed the advantages of different authentication and secure key management systems. However, they did not cover the real-time review framework [11].

Oberoi et al. introduced an enhanced security approach against blackhole attacks in VANETs using a Flag status-based technique. While this framework improves the quality of Service parameters, it comes with increased computational complexity [12].

Zhang et al. presented a lightweight system that combines message recovery with a signature method for message authentication with reduced communication overhead. Although its security outcomes are promising and are aimed at achieving low transmission delays, there is a need for further adjustment regarding sensitivity [13].

Verma et al. introduced the Elliptic Homomorphic Signature system to ensure the legitimacy of trademark usage in VANETs. This system uses a secret key to create signatures when users sign and encrypt data. Only authentic users can generate signature products, and data integrity is confirmed by the destination using the public key. While effective and secure, this structure is deemed inappropriate for real-time networks [14].

Zhou et al. proposed a privacy-preserving identity authentication system based on the certificate-less aggregate signature technique. This system allows users to create

fuzzy identities to conceal their true identities while maintaining the same private key even when modifying their pseudonyms. The protocol avoids bilinear mapping to enhance computing efficiency but may not be suitable for real-time scenarios [15].

Yang et al. introduced an Nth degree Truncated polynomial Ring Unit-based key negotiation and authentication protocol that offers certificate-free authentication, mutual authentication, and user anonymity protection. This protocol withstands quantum attacks, complies with various security standards, and performs well in terms of computing and communication overhead. However, the framework's sensitivity remains a concern [16].

Showkat et al. introduced a lightweight VANET authentication using cuckoo filters, reducing CRL verification costs. It resists attacks like impersonation, replay, and man-in-the-middle with lower authentication overhead, but introduces more latency [17]. A 3-tiered trust management system was proposed by Jyothi et al. to address hostile vehicles, which assigns trust ratings based on vehicle characteristics. This system enhances data packet transmission rates and reduces source-to-destination latency in the presence of malicious vehicles. However, sensitivity analysis is limited [18].

Yuxin et al. introduced an adaptive immune approach using immune nodes to prevent the spread of worms more effectively. However, the sensitivity of the system's key is relatively low [19]. Da L et al. utilized a cloud server and a trusted authority (TA) to monitor road conditions. Hence, the reports regarding road conditions can only be uploaded to the cloud server by authorized vehicles. While this system protects road condition reports for security and privacy, it raises computational challenges [20].

In summary, many key generation-based encryption techniques in VANETs require substantial resources and are susceptible to powerful attacks at different node levels. The proposed NC-HLM model addresses these challenges by creating cryptographic algorithms at the RSU end, allowing OBUs to perform encryption.

3 Proposed Methodology

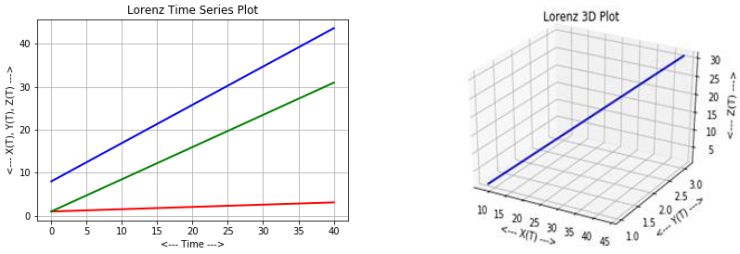
The suggested method uses hybrid Henon-Logistic maps to transmit data from OBU to RSU. This transmission involves utilizing inputs such as the authenticator, the vehicle's information, and the engine's diagnostic data as integral components of the authentication process. The preceding section delved extensively into the intricate workings of each individual module within the system.

3.1 Proposed Encryption Models

3D logistic chaotic maps exhibit a higher degree of chaos. The mathematical expressions for this enhanced chaotic behavior are specified below, subject to the conditions: $\alpha = 0.0015$, $\beta < 0.0022$, and $0.35 < \mu < 0.381$. The logistic map characteristics shown in Fig. 1 visually demonstrate the chaotic phenomenon associated with the recommended 3D chaotic system operating under the aforementioned parameter settings.

$$X = \mu x\big(1 - x(i)\big) + \beta y' X + \alpha Z \tag{1}$$

$$Y = \mu y\big(1 - y(i)\big) + \beta x' Z + \alpha Y \tag{2}$$
$$Z = \mu z\big(1 - z(i)\big) + \beta z' y + \alpha X \tag{3}$$

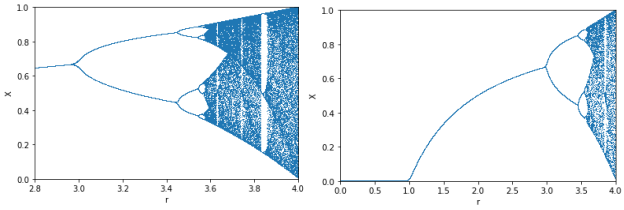


(a) (b)

Fig. 1. Demonstration of chaotic phenomenon (a) series plot (b) 3D plot

The mathematical formulation of the 2D Henon map, which is an invertible chaotic system, is provided below with the bifurcation parameters a and b. In this context, it's important to note that the contraction factors remain independent of both the x and y variables. In order to achieve a chaotic state the bifurcation boundaries have been determined to be 0.3 and 1.4 through multiple experiments. Bi-periodic oscillations are generated when the 0.85 < a < 1.1, and the two bifurcation functions are merged. The same is represented in Fig. 2 with the necessary initial conditions.

$$x_{(n+1)} = 1 - ax_n^2 + y_n \tag{4}$$
$$y_{(n+1)} = bx_n \tag{5}$$



(a) (b)

Fig. 2. Bifurcation characteristics of 2D Henon map

3.2 Encryption Mechanisms for NC-HLM

The proposed method enhances the security of the vehicle network by offering a robust encryption technique that safeguards against security threats. Here are some of its key characteristics: (1) Secure Data Exchange: This method ensures secure data exchange between vehicles and the RSU, protecting the integrity and confidentiality of the transmitted information, (2) Dual primary Secret Keys: It employs communication (Ec) and

encryption (Ek) secret keys during the initial phases of communication. These keys are constructed with chaotic properties, leading to continuous updates at predefined intervals. Importantly, the keys are never shared over the network but they are retained within the gateway and the devices, (3) Unique Lightweight Protocol: The method utilizes a unique and lightweight protocol based on the concept of logistically based Henon chaotic maps. It leverages network metrics such as distance (D), Channel ID, and Received Signal Strength Indicator (RSSI) to establish initial conditions for OBUs. As a result, the generated keys exhibit a high level of unpredictability, enhancing security. In summary, this approach not only enables secure data exchange but also employs dynamic and robust key management techniques based on chaotic maps to enhance the security of the vehicle network, making it resilient against potential threats.

3.3 Key Generation Process

Network characteristics of OBUs are initially assessed, followed by the construction of logistic maps based on various parameters of the OBUs. These maps serve as the foundation for generating high-complexity encryption keys. In the first level of key generation, the monitored network parameters are RSSI, Distance between the OBU and RSU (D), and Channel ID. The distance between nodes and gateways is computed using the RSSI formula with P_o and P_r as signal power in zero distance and distance d, frequency(f), and path-loss exponent (n).

$$D_{(N_s,BS)} = 10\left[\frac{(P_o - F_m - P_r - 10n\,log(f) + 30n - 32.44)}{10n}\right] \tag{6}$$

Network parameter measurements serve as the foundational data for chaotic scroll map generation. Table 1 highlights the RSSI values experimentally measured by employing transceivers interfaced with IoT device microcontrollers.

Table 1. Received Signal Strength Indicator characteristics determined.

S. No	RSSI (dbm)	D (meters)
1	-98 to -84	6
2	-88 to -78	5
3	-76 to -72	3

Upon calculating the network parameters, the first level involves the generation of highly complex keys, which then act as inputs for Henon Maps. In this proposed protocol, a diffusion operation is employed to create new keys with high randomness, enhancing the overall security of the system with I (OBUs sensor values) and chaotic matrix values X, Y, Z.

$$E_k = D\big(I, NCLH(X, Y, Z)\big) \tag{7}$$

4 Results and Discussion

The primary objective of encryption techniques is to introduce randomization into the key generation process. NIST has established certain assessments for randomness evaluation to ensure the suitability of the random or pseudo-random generator for cryptographic applications.

Frequency Mono-bit Test: The described test assesses whether a sequence of ones and zeros exhibits patterns resembling real data. The test value measures how closely the proportion of ones in the sequence aligns with half of the total sequence length. In this test, ones are represented as +1, while zeros are represented as -1. The iterative frequency mono-bit testing yields several parameters, as outlined in the list. Table 2 demonstrates this for the NC-HLM scheme over a 5-cycle period exhibits randomness while also meeting the encryption requirements necessary to withstand significant attacks. This validates the suitability of the proposed method.

Table 2. Mono-bit test observations for the proposed system.

Iterations	Test type	Decision rule	Randomness assessment	Key Test
1			P=0.0872900	
2			P=0.0564313	
3			P= 0.0445343	
4	Frequency		P=0.0325721	PASS
5	Mono-bit	P>0.01	P=0.0468963	

Frequency Block Test: This test divides the encryption key of k-bits into two equal parts containing k/2 bits, for each repetition. The key is then evaluated in this scenario, and it is considered acceptable when the P>0.01. Table 3 highlights the results obtained.

Table 3. Inferences of Block Test on the suggested system.

Iterations	Test type	Decision Rule	Randomness assessment	Key Test
1			P=0.0302920	
2			P=0.0433445	
3			P=0.0426233	
4	Frequency		P=0.0523002	PASS
5	Block bit	P>0.01	P=0.0442103	

Run Test: This test examines all available runs continuously until a different bit sequence interrupts the run. Table 4 presents the results for the NC-HLM scheme. In this experiment, the oscillations, which are considered transitions from ones to zeros, were observed to occur most rapidly in V(n)(obs). This observation indicates that the suggested NC-HLM model indeed generates significant randomness, as intended.

Table 4. Observations of run test for the proposed system.

Iterations	Test type	Decision Rule	Randomness assessment	Key Test
1			P=0.0312681	
2			P=0.0478292	
3			P=0.0539083	
4	Run test		P=0.0454124	PASS
5		P>0.01	P=0.0334679	

Longest Run Test: This run test is utilized to identify the length of completed runs within an M-bit sequence. Presented below are the results in Table 5, which illustrate the examination of irregularities detected by the model across different M-values in accordance with NIST standards. Table 6 outlines the outcomes of this test specifically for the proposed scheme.

Table 5. Observation for varied sequences

Min. n sequence	Max. M values
128	8
6272	128
750,000	10^4

Table 6. Results for the proposed scheme

Iterations	N	N1	N2	D1	P	Key test
1	256	42	67.3	-1.415298	0.054789	
2	256	43	65.5	-3.6832	0.068912	
3	256	28	76.0	-5.7890	0.057893	
4	256	31	54.0	-1.83536	0.065234	
5	256	30	78.0	-4.890	0.048799	PASS

Key Sensitivity: When examining the pseudo-randomness in chaotic systems, it's important to note that dynamic systems demonstrate significant sensitivity. This sensitivity is harnessed to securely encrypt data transmitted between devices. Notably the suggested model (NV-HLM) exhibits greater randomness than the existing single chaotic AKA scheme [21] as depicted in Figure 3.

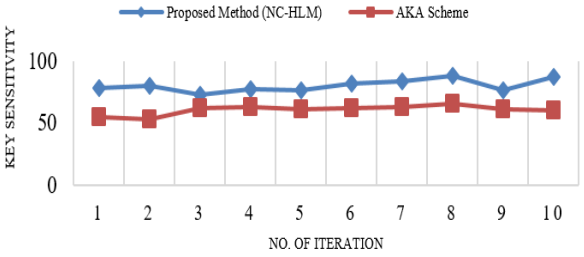


Fig. 3. Comparative analysis on key sensitivity.

Discrete Fourier Transform (DFT) Test: The aim is to assess if crest frequencies above the 95% threshold significantly differ from 5%. Table 7 displays DFT results for NC-HLM. To confirm randomness, P>0.01, and D should be smaller.

Table 7. Inferences from the DFT test

Iterations	N	N1	N2	D1	P	Key test
1	256	38	67.3	-2.456298	0.046472	
2	256	43	65.5	-4.5890	0.068664	
3	256	45.3	76.0	-7.46789	0.079845	
4	256	45	54.0	-1.8930	0.057538	

5	256	47.2	78.0	-4.5789	0.036787	PASS

BAN technique: The security strength of the suggested system was tested using the BAN technique, which assesses data integrity and protection against attacks. BAN is a trusted validation method for demonstrating mutual authentication. We developed an ideal message format and conducted BAN-logic proofs, systematically verifying the protocol's security. After 16 phases, we successfully achieved the predefined goals, confirming the protocol's strong performance and reliability.

5 Conclusion

The paper addresses the increased vulnerability of VANETs to cyber issues due to the chaotic nature of data transmission. To mitigate these risks, hybrid Henon map-based encryption methods are employed. These chaotic encryption algorithms employ random key generation to encode data securely. The suggested NC-HLM model contributes to generating highly logical pseudorandom codes for data transmission. The proposed technique underwent evaluation against NIST standards, demonstrating its effectiveness in defending against attacks. The system was also examined for the efficiency and structure of its encryption schemes.

References

1. Ala Al-Fuqaha, Ammar Gharaibeh, Ihab Mohammed, Sayed Jahed Hussini, Ab-dallah Khreishah, and Issa Khalil. Online algorithm for opportunistic handling of received packets in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 20(1):285–296, 2018.
2. Gongjun Yan and Stephan Olariu. A probabilistic analysis of link duration in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 12(4):1227–1236, 2011.
3. Chung-Ju Chang, Ray-Guang Cheng, Hao-Tang Shih, and Yih-Shen Chen. Maximum freedom last scheduling algorithm for downlinks of dsrc networks. *IEEE Transactions on Intelligent Transportation Systems*, 8(2):223–232, 2007.
4. Jeong-Kyu Bae, Myung-Chul Park, Eun-Ju Yang, and Dae-Wha Seo. Implementation and performance evaluation for dsrc-based vehicular communication system. *IEEE Access*, 9:6878–6887, 2020.
5. Chuan Xu, Zhengying Xiong, Xianghui Kong, Guofeng Zhao, and Shui Yu. A packet reception probability-based reliable routing protocol for 3d vanet. *IEEE Wireless Communications Letters*, 9(4):495–498, 2019.
6. Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems*, 16(6):2985–2996, 2015.
7. Ikram Ali, Tandoh Lawrence, Anyembe Andrew Omala, and Fagen Li. An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in vanets. *IEEE Transactions on Vehicular Technology*, 69(10):11266–11280, 2020.

8. Jie Cui, Jing Zhang, Hong Zhong, and Yan Xu. Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter. *IEEE transactions on vehicular technology*, 66(11):10283–10295, 2017.
9. Guanjie Li, Chengzhe Lai, Rongxing Lu, and Dong Zheng. Seccdv: A security reference architecture for cybertwin-driven 6g v2x. *IEEE Transactions on Vehicular Technology*, 71(5):4535–4550, 2021.
10. Shengke Zeng, Yuan Huang, and Xingwei Liu. Privacy-preserving communication for vanets with conditionally anonymous ring signature. *International Journal of Network Security*, 17(2):135–141, 2015.
11. B Manimekala, KS Divya, and Sreeparna Chakrabarti. A study on secured data transmission, key management and its comparative analysis of scheduling techniques in vanet. *In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, pages 283–288. IEEE, 2021.
12. Vibha Oberoi. Enhancement of qos in security algorithm for blackhole attack in vanet. *In 2020 IEEE Pune Section International Conference (PuneCon)*, pages 33–37. IEEE, 2020.
13. Jianhong Zhang and Qijia Zhang. Comment on secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in vanets. *IEEE Transactions on Information Forensics and Security*, 18:1037–1038, 2023.
14. Raman Verma. An efficient secure vanet communication using multi authenticate homomorphic signature algorithm. *In 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pages 1–5. IEEE, 2023.
15. Yanwei Zhou, Lei Cao, Zirui Qiao, Zhe Xia, Bo Yang, Mingwu Zhang, and Wenzheng Zhang. An efficient identity authentication scheme with dynamic anonymity for vanets. *IEEE Internet of Things Journal*, 2023.
16. Jiayu Yang, Fei Li, and Zhuoran Zhang. Research on ntru-based anonymous authentication and key negotiation protocol for vanets. *In 2022 7th International Conference on Cyber Security and Information Engineering (ICCSIE)*, pages 104–108. IEEE, 2022.
17. Shafika Showkat Moni and D Manivannan. A lightweight privacy-preserving v2i mutual authentication scheme using cuckoo filter in vanets. *In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 815–820. IEEE, 2022.
18. N Jyothi and Rekha Patil. A multi-tier accredit based security for trustworthiness in vanet's using broadcasting mechanism. *In 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEE-ICT)*, pages 1–7. IEEE, 2023.
19. Ding Yuxin, Huang Ningxin, and Xu Wenting. A dynamic immune strategy for blocking the spreading of worms in vanets. *In 2022 International Conference on Machine Learning and Cybernetics (ICMLC)*, pages 97–102. IEEE, 2022.
20. Lemei Da, Yujue Wang, Yong Ding, Bo Qin, Xiaochun Zhou, Hai Liang, and Huiyong Wang. Cloud-assisted road condition monitoring with privacy protection in vanets. *In 2022 18th International Conference on Mobility, Sensing and Networking (MSN)*, pages 304–311. IEEE, 2022.
21. Lu Wei, Jie Cui, Hong Zhong, Yan Xu, and Lu Liu. Proven secure tree-based authenticated key agreement for securing v2v and v2i communications in vanets. *IEEE Transactions on Mobile Computing*,

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.