International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

VANET Communication System with HENON Based Privacy Preserving Authentication

M. S. Bennet Praba[1], S. S. Subashka Ramesh[2]

Submitted:22/03/2023 **Revised:**28/05/2023 **Accepted:**10/06/2023

Abstract: It is extremely difficult to ensure the security of the Vehicular Internet of Things (VIoT) because of how diverse and infrastructure-free it is deployed, which exposes it to a variety of security concerns. There is an urgent need for a mutual authentication method among the linked devices to solve this problem and safeguard sensitive data inside the deployed region. However, when used in VIoT systems, previous methods have significant computational costs and insecure connectivity. Therefore, it is essential to provide an authentication system that protects privacy and can successfully protect VANET devices from attacks. In order to provide private and secure authentication between VANET devices, this study offers a special, compact, and secure protocol based on network-centric Henon Chaotic Maps (NC-HCM). The proposed method enables real devices to vary their keys for each transmission iteration while ensuring secure transmission of sensitive data from the source to the destination. The security level of the proposed model is assessed and analysed formally using the Burrows-Abadi-Needham Logic (BAN). The given model is also thoroughly verified using AVISPA and the Profverif tool. The results of the investigation show that the suggested strategy acts as a strong deterrent against both active and passive attacks. It successfully protects the VANET devices and guarantees the veracity, integrity, and secrecy of the data sent.

Keywords*: Embedded VANET devices, Henon-Chaotic Maps (HCM), Network Centric, PBC, and BAN*

1. Introduction

VANET (Vehicular Ad-Hoc Network) has seen phenomenal rise in popularity over the past 20 years and has attracted a lot of attention. Intelligent agriculture, disaster prevention, military surveillance, medical treatment, and manufacturing automation are just a few of the real-world applications for it that exist [1-3]. This is because of its versatility. The concept of a VANET has grown over time, incorporating advancements that make it suitable for a range of businesses and tasks. Healthcare infrastructure is one major area where VANET has had a big impact. VANET-based systems provide for the efficient monitoring of patients' vital signs and the facilitation of their care [4]. This development has created new opportunities for improved healthcare delivery and remote patient monitoring.

Because of this, VANET in healthcare has become a significant and well-known development in the medical industry. To manage the massive volume of varied data and sensor inputs, sensitive data collected from VANET devices is stored in a cloud database. Due to the fact that this data contains sensitive medical information, maintaining its privacy and security is crucial [5-7]. As a result, data saved in private cloud databases cannot be accessed by unauthorised parties, guaranteeing its anonymity.

Various security flaws including fraud, espionage, and falsification can put the safety of cloud services and devices at danger. Both bad insiders and outside attackers have the potential to take advantage of these vulnerabilities [12]. Although current methods [8–11] have shown that these attacks may be successfully defended against with appropriate defensive algorithms, it is still vital to be on guard. Additionally, some VANET hardware elements, such IP cameras and smart speakers, are prone to attacks like the Mirai malware [13]. A serious threat to the internet infrastructure, particularly VANET-based medical environments, is posed by the existence of such malware [14–16]. To safeguard the integrity of important medical environments and safeguard VANET systems from potential harm, it is imperative to address these vulnerabilities and apply the necessary security measures.

It is essential to build complete solutions that cover end-device security, message verification, authorization, authenticity, security, loss of service security, accessibility, and privacy safeguards in order to meet the problems that VANET systems confront [17]. To enable a number of security measures, it is crucial to establish a strong authentication mechanism. The first line of defence is authentication, which stops both passive and aggressive attacks. Mutual verification and session-key agreement are

[1]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, BharathiSalai, Ramapuram, Chennai, 600089, India*
[2]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, BharathiSalai, Ramapuram, Chennai, 600089, India*
** Corresponding Author: 1.M.S.Bennet Praba, Email: bennetms09@gmail.com*
2. S.S.Subashka Ramesh, Email:subashka@gmail.com

two essential responsibilities that a successful authentication system should satisfy. The confirmation of entities or devices requesting access to the private cloud platform is ensured by these roles. In authentication systems, robust encrypted communications are frequently used to establish mutual validation, session-key agreement, and to thwart security invasions. In order to choose the most effective encryption technique, consideration must be given to variables including power consumption, sensor and device setups, and encryption method choice.

Therefore, it is essential to adapt encryption techniques within a suitable authentication protocol to meet the needs of the VANET devices and sensors. Existing research has tried to meet this need by developing simple authentication techniques based on chaos theory and symmetric key cryptography. However, these protocols usually incur high operational costs, energy consumption, and memory usage. This paper suggests an innovative and lightweight mutual authentication method based on network-centric Henon Chaotic maps to get over these restrictions and guarantee a high level of security for sensitive clinical data. In comparison to current methods, the suggested model improves algorithm efficiency and performance by incorporating bio-inspired and optimised chaotic systems. The following is a summary of the main contributions of this research study:

This study introduces a novel, lightweight authentication method with strong defensive properties. In order to achieve a high level of unpredictability, it uses a hybrid strategy based on network-centric hash scroll maps that are optimised using network parameters.

The communication costs for various types of VANET devices are estimated in order to evaluate the effectiveness of the suggested methodology. Based on this metric, the operating cost of the scheme is calculated and contrasted with more advanced techniques. The comparison shows that the suggested plan has a more lightweight design and better cost effectiveness. Furthermore, an informal security analysis based on mathematics supports its effectiveness [20]. In terms of resilience, effectiveness, and security against both active and passive threats, the evaluation and comparison of the proposed technique to existing schemes demonstrate that it outperforms them [21]. The proposed plan also successfully accomplishes the goal of maintaining strong privacy.

The rest of the essay is organised as follows: Section II talks about the many authentication methods that have been proposed by different authors. Section III presents Henon maps as background information. The key generation and authentication procedures as well as the suggested model's operational mechanism are thoroughly discussed in Section IV. A comparison study and an experimental validation of the security analysis are presented in Section V. The final section of the document before it is done is future enhancements.

2. Literature Survey

A communication protocol based on group organisation was presented in a study by H. El Hadj Kalil et al. For each group of cars in this architecture, a group leader known as the master is chosen. The only entity permitted to communicate with a Roadside Unit (RSU) is the master. The main advantage of this architecture is that it improves network performance by reducing the stress on the master. It also effectively manages the tag's increasing processing burden. The drawback of this structure is that it requires more time for processing [22].

In a study by Z. Wei et al., an identity-based signature method without the need of a random oracle was suggested as being immune to chosen-message assaults. By creating effective outsourcing algorithms for exponential operations, this framework aims to lower computing costs. A homomorphic mapping based on matrix conjugate operations was used to guarantee the security of both exponents and base numbers. However, as indicated in [23], this technique has a disadvantage in that it has a larger communication overhead.

A blockchain-based authentication handover method for VANETs was introduced by S. Son et al. To maximise network efficiency in this framework, vehicles make quick computations during handoffs. The system's robustness is demonstrated by the fact that it uses little computer power while successfully detecting harmful activity. The model also exhibits simplicity of use and necessitates little communication [24].

Hash functions and exclusive-OR operations are used in the communication architecture that X. Li et al. claimed as being specifically created for VANET. They presented a compact authentication technique that successfully responds to the demand for privacy protection. It is shown that this protocol accomplishes the specified security objectives through a formal security analysis utilising BAN logic. The technique has a number of benefits, including increased security, efficacy, social awareness, and lower computational costs. It should be emphasised, nonetheless, that sustaining its performance might call for more resources [25].

A. Mansour et al. present ALMS, a revolutionary group key management protocol. By acting as a middleman between users and the VANET environment, this protocol makes sure that users can only join after passing through several authentications. Even if a hacker is successful in recovering the secret key but is unable to access the inactive authentication keys, the system ensures security for the authentication process. This framework does not

cover real-time frameworks despite its primary focus on authentication techniques [26].

R. I. Abdelfatah et al. propose a novel authentication scheme that enables safe communication between cars and infrastructure, replacing secure channels with Chebyshev chaotic maps. This protocol presents a revolutionary network paradigm with little hardware complexity. However, it should be noted that this framework's primary drawback is how time-consuming it is [27].

M. Umar et al. suggest a simple VANET authentication system that ensures private data transfer over a public channel while maintaining efficiency and security. Lower communication and computation costs, which improve communication efficiency and save time, are a defining feature of this protocol. It should be emphasised, though, that this technique raises the cost of authentication [28].

Secret Sharing, a Physical Unclonable Function (PUF), is used by W. Othman et al. as a safe and private message authentication method. The security and privacy are both guaranteed by this protocol, which successfully defends against passive and active attacks, including memory leaking. Energy-saving effects are achieved by using energy-efficient lightweight crypto modules. The added latency that could result from each edge or fog node independently authenticating the devices, which is not ideal for real-time services, is a potential disadvantage of this strategy [29].

For location-based services (LBS) in VANETs, J. Zhou et al. suggested a simple authentication scheme that preserves privacy. They developed a useful information filtering system that protects privacy and enables encrypted LBS communications before authentication. Faster authentication times are provided by this architecture [30]. But it should be highlighted that when data sizes grow, so do connection costs, which is one of the main drawbacks of this strategy.

A unique V2I authentication technique named PLVA was introduced by S. Lv et al. It prioritises privacy and performs well. This method enables quick authentication between cars and RSUs over their entire travel by utilising data from inferred RSUs. The framework offers highly secure and affordable computing, which helps to increase energy efficiency and lower costs. It's crucial to remember that the system's main disadvantage is communication overhead [31].

An authentication scheme for VANET that prioritises extremely low transmission latency and transmission cost was proposed by J. Zhang et al. Their solution achieves message authentication by combining a signature technique with message recovery, which lowers communication overhead. With this framework, memory usage, computational efficiency, and communication efficiency are all enhanced. The communication cost of the longest message sent via this protocol is 872 bits, which is deemed acceptable. The biggest issue with this technology, though, is its energy usage [32].

3. Pre-Requisties

In this part, the basic principles of henon maps are discussed.

3.1 An overview of the Henon maps

LevHenon maps [33], which are produced by its defining equation, are disruptive quadratic and non-linear maps.

$$Yn+1=1-bXn \quad (1)$$

$$Xn+1=1-aXn2+Yn \quad (2)$$

The classification of a map as a classical map depends on the values of its parameters, a and b. Henon's map deviates from the conventional norms and behaves chaotically when a = 1.4 and b = 1.3. Henon maps exhibit chaotic behaviour, which may be seen by performing iterative tests with various values of a and b. Figure 1 illustrates the chaotic behaviour of henon maps using common values for parameters.

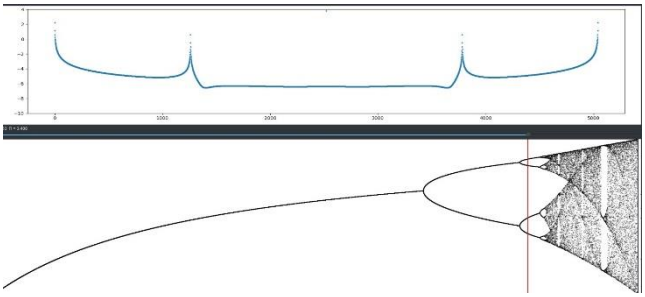

Fig 1. Properties of Henon maps'

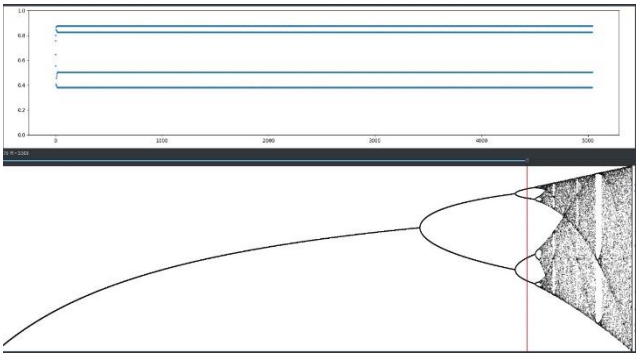

Fig 2. Properties of Henon maps'

4. Suggestive Procedure

4.1 System Overview

In order to increase the security of the VANET network, the proposed protocol offers a secure method for authenticating users, Roadside Units (RSUs), and Vehicle

Ad-Hoc Network (VANET) hardware. Between sensors, RSUs, and users, intermediary RSUs are deployed in the system model. The protocol has a number of benefits, one of which is the creation of a safe mutual authentication system between RSUs and VANET hardware. The communication key (Ec) and the encryption key (Ek), two essential secret keys, are used to accomplish this. These keys are used at various stages of mutual authentication. The keys have chaotic properties that increase security and cause constant changes after a predetermined session length. Additionally, all configuration-related keys are solely kept in hardware and RSUs, preventing any interchange of them through networks.

The suggested protocol presents a novel and flexible way of authentication based on scroll-based Henon chaotic maps. To determine the initial parameters for key generation, VANET devices use three network metrics: Received Signal Strength Indicator (RSSI), distance (D), and Channel ID. With this strategy, a produced key is guaranteed to be highly unpredictable, providing good protection against unauthorised access and data theft. The addition of this security layer significantly strengthens the network as a whole and provides protection against upcoming intrusions.

The system's overall security is strengthened by this integration. Additionally, the proposed protocol has been designed to reduce energy consumption and message exchange time while carrying out mutual authentication and data transfer. Table 1 offers a comprehensive list of all acronyms used in this study for your convenience.

Table 1. List of Terms Abbreviated in the Article

Symbol	**Explanation**
E_k	The VANET devices and RSUs store the permanent encryption key.
E_c	Each and Every Session's Key Updated
E_i	the initial key for the update
$Session_{(T+1)}$	Time of the session for the subsequent key update
$Seq_{\{i\}}$	For the session time-key update, a random sequence was created.
$Seq_{\{i+1\}}$	created randomly for the session's time-key update at position i+1
L	Key duration
T1, C2	For each task, random sequences are created.
NCSH	Network-focused scrolling Henon maps

4.1.1 Technique for generating keys

Network-centric improved scroll chaotic sequences are built to generate highly complicated keys. VANET devices' network metrics, such as RSSI, distance, and Channel ID, are measured. These parameters from various VANET devices are then used to produce scroll chaotic attractor maps.

The first level chaotic keys are evaluated based on these network properties.

The most frequent term used in calculations between nodes and RSUs is the RSSI (Received Signal strength Indicator, or RSUs), abbreviated as RSSI (R).

The user transceivers that interfaced with the node had a channel ID.

Following the computation of the network parameters, high complex keys are generated at the first level and utilised as the inputs to the Henon Maps. The suggested method generates new keys with high levels of randomness using the diffusion process. The flowchart for the complete key generating procedure is shown in Figure 5.

The mathematical procedure underlying the suggested key generation is described in detail.

First step: The initial conditions for the Henon maps have been created. In this case, the proposed research makes use of a random estimate of a VANET network's attributes. Three-dimensional logistic maps' initial conditions were generated utilising elements like distance (D) and received signal strength (RSSI). The section contains instructions on how to measure RSSI and distance.

Next, focus on networks Henonmaps are generated based on the stated fundamental parameters. The memory areas of the VANET devices house these scroll maps. These are regarded as the inputs to the Henon maps.

Step 3 Henon Chaotic maps are produced using the scroll matrix, as described in Steps 2 and 3.

Step 4: The unique hybrid NCH maps and the sensor data from the VANET devices are diffused (D) to create the high randomness key (Ek).

The Device ID and RSU ID are distributed to build the accompanying hash messages in Step 5 using network-centric NCH maps. These values have been adjusted to the address length L of VANET devices due to the size variations between IDs and chaotic matrices.

HashDevice ID=DDevice ID ,NCHX,Y,Zscaled to L

HashGateway's ID=DGateway's ID ,NCHX,Y,Zscaled to L

4.2.Privacy Preserving Authentication Phases:

The three stages that make up this phase are as follows, with discussion:

4.2.1 RSU with VANET devices

The network's VANET devices start the mutual authentication procedure by sending the hashed device ID and a randomly generated challenge T1 to the RSU. Using a key called Ek, the initial authentication message is encrypted. To guarantee message integrity and authenticity when sending the entire message, each VANET device computes the RSSI and makes use of the first update key.

4.2.2 RSU to VANET hardware

The RSU decrypts the message after receiving it from the VANET device and compares the hashed ID it receives to the hash IDs it has already saved. If they do, the authentication procedure is then carried out, which involves calculating the RSSI for the entire message. The authentication procedure fails if the IDs are different. If the predicted RSSI satisfies the threshold RSSI criterion, the RSU checks the VANET devices. It chooses Seqi, a string of integers, together with C2, a freshly produced challenge, N1, Session(T), the predetermined session duration, and Hash(Device ID), which will be used to update the session key. The key Ek is used to encrypt each of these values. The RSU then uses the key Ec to calculate the RSSI (msg2) and sends it to the VANET device.

4.2.3 VANET-Devices -→ RSU:

The VANET device receives message 2 from the RSU, decrypts it, and compares the received hash of the RSU's ID to the previously stored hash. The authentication procedure proceeds if the two hashes are identical. After then, the RSSI is contrasted with the threshold RSSI. The VANET device authenticates the RSU and certifies that the RSU made the right choice for data transfer if the received RSSI is equal to the threshold RSSI. The authentication, however, fails if the obtained RSSI does not coincide with the threshold RSSI. For the full message, the VANET device calculates the hash of C2, random sequences Seqi+1, session time Session(T+1), and RSSI. To ensure that the RSU has successfully received the message from the VANET device, these values are encrypted using the key Ek and sent to it.

The RSU decrypts message 3 after receiving it from the sensor and confirms that the device's hashes match. The authentication fails if the hashes do not match. The RSU calculates the RSSI for the message it has received and compares it to the RSSI value received if the hashes match (RSSI(msg3) = [RSSI(T)(msg3)]rec). The RSU authenticates the VANET devices if the computed RSSI and the received RSSI are identical. Due to message 3, the RSU is aware that the VANET devices have C2, random sequences Seqi+1, session time Session(T+1), and RSSI. The acknowledgment (ACK), the RSSI(msg4), and the encrypted hash of the RSU's ID are sent to the sensor. The shared secret key, Ek, is utilised by the RSU for encryption. The RSU can use this procedure to check if it got message 3 from the VANET devices properly.

5. Analysis Theoretical of Proposed Protocol

To assess the robustness of the suggested protocol, a theoretical security analysis is carried out in this section. Highly random keys are used to boost the security of the protocol, which also increases its robustness. The protocol can fight against many attacks, including Man-in-the-Middle, Brute Force, and impersonation assaults, according to the security analysis.

5.1 MIM

A "man-in-the-middle attack" (MIM) is a form of security breach in which an active attacker actively intercepts and tampers with data being sent between two parties in a communication channel. The communication may be seriously compromised as a result of this. In the proposed protocol, an attacker would need access to the encryption keys in order to decode and alter the data when intercepting communication between VANET devices. The protocol, however, employs wildly unpredictable and disorganised keys for encryption, making it extremely unlikely for an attacker to derive any useful information from the intercepted conversation. Furthermore, attackers are unable to gather all the required keys to decode and change the data because there are two distinct chaotic keys utilised and these keys are never broadcast over the network. As a result, the recommended approach successfully foils man-in-the-middle assaults.

5.2 Brute Force Attack

A Brute Force Attack involves the attacker repeatedly attempting various secret keys or passwords in an effort to decrypt the connection. For the reasons listed below, the suggested protocol offers strong defence against brute force attacks. First of all, it is quite difficult to utilise a brute force method to uncover the keys because of how unpredictable they are. Keys also stay hidden and inaccessible to potential attackers since they are never communicated over the network but are instead safely held in the memory of VANET devices and RSUs. Finally, an attacker cannot start or influence the mutual authentication process because it is carried out on the backend of the communication channel. The suggested protocol provides protection against brute force assaults as a result.

5.3 Impersonation Attack

Attacker attempts to pass for another genuine user node during impersonation attack. If the attacker wants to repeat themselves, they must comprehend each stage of the mutual authentication system that they are unable to discover. Therefore, the proposed protocol can tolerate impersonation attempts.

5.4 Data Integrity and Confidentiality

Data integrity guarantees that communication is duplicate-free, error-free, unaltered, and in the proper order during transmission. Through the use of the NCSH process, the proposed research integrates both data integrity and confidentiality. An attacker would need to compromise the dynamic chaotic chain built between the sender and recipient in order to tamper with the transmitted messages, which presents a substantial hurdle. Thus, the suggested protocol successfully maintains data integrity and secrecy while protecting the communication from unauthorised access and modification.

5.5 Replay Attacks

In order to establish an authenticated session, an attacker listens in on reliable communications being sent and received and then replays the data.

6. Experimental Validation

This section examines security and lightweight qualities using the Communication Cost and BAN-logics. Furthermore, the suggested protocol's level of security is examined using AVISPA and other tools.

6.2 Communication cost

The authentication process shown in Figure 3 and the sensor inputs are used to calculate the communication cost, which is then multiplied by the embedded microcontroller's operating range of 5 to 10. It's vital to remember that before being sent to the intended recipient, all authentication credentials used in this study are hashed and encrypted. Thus, the amount of data communicated during the authentication procedure determines the transmission cost.

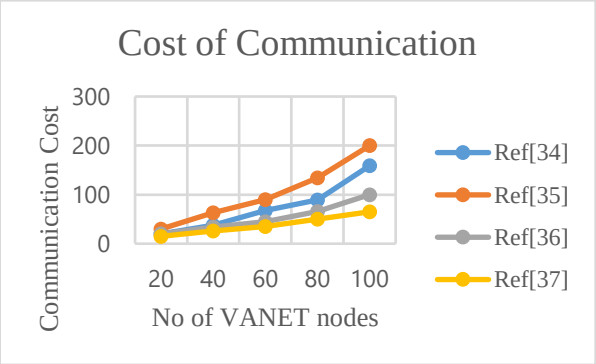

Fig 3 Analysis of Communication Costs for Each Authentication Protocol with Privacy Preserving

6.3 BAN Security Proof Analysis

Burrows, Abadi, and Needham created the BAN logic, which offers a set of recommendations for creating and assessing information exchange protocols. The BAN logic aids protocol designers in proving the security of their protocols by looking at the dependability and protection of the sent information [35]. A well-known method for examining the precision and mutual authentication of authentication protocols is BAN logic. In this study, before beginning the BAN logic analysis, we specified four very explicit goals. We defined the idealised message format and provided the presumptions for the BAN logic proof. Following the BAN logic's tenets, the suggested protocol's security was carefully shown over the course of 16 phases. After doing this investigation, we were able to accomplish the predetermined goals, demonstrating the validity and suitability of the suggested solution for VANET environments. The suggested protocol is also appropriate for networks with limited resources. Different BAN logic notations were used to make the BAN logic analysis easier, and Table 2 documents how they were used in this study. An outline of the BAN logic analysis process, which was used to confirm the proposed protocol's security, is provided below.

Table VII Symbols for BAN-logic

Notation	Explanation
Pr|≡A	Presumes A is Correct
Pr◁A	Pr gets a message with A in it.
Pr|~A	A telegram from Pr once contained A.
Pr⟹A	Pr has authority over A.
#(A)	Before this round, A was not sent as part of a message.
Pr⟷k Qr	K can be used by Pr and Qr to converse.
A,Bk	Combining A and B

6.3.1 BAN Logic Formulas

Formula used are

Res1:Pr|≡#(A)Pr|≡#(A,B)

Res2:Pr|≡#A, Pr|≡Qr|~APr|≡Qr|≡A

Res3:Pr|≡Pr⟷k Qr , Pr◁(A)kPr≡Qr~A

Res4:Pr|⟹A,Pr|≡Qr|≡XPr|≡#(A,B)

Res5:Pr|≡A,Pr|≡YPr|≡(A,B)Pr|≡Qr|≡(A,B)Pr|≡Qr|≡A

6.3.2 Goals for Security

Ek=NCSH(C1,C2,Kc)

Ek and Kc have been negotiated in advance

The goal is assumed to be achieved through the following security objectives.

goal1:S|≡S↔N1, N2RSU

goal2:S|≡G≡S↔N1, N2RSU

goal3:G|≡S↔N1, N2RSU

goal4:G|≡S|≡S↔N1, N2RSU

6.3.3 The Perfected Shape

The ideal message exchange looks like this:

Message 1: Sid, SNRSU (SG)

Message 2: Gid, SNG1, SNG2SKp KikG

Message 3: Sid, SNG1, and SNG2 SKp, KikG

Message 4: Gp, KikG:S:(Gid, ACK)S

6.3.4 The Proving Process for BAN-Logic

Process for Logic Proof: Here is how the BAN logic Proving method is explained..

Begin

Initialization

P1:S|≡#(C1)

P2:G|≡#(C2)

P3:S|≡S↔Ek, EcG

P4:G|≡S↔Ek, EcG

P5:S|≡G⇒S↔ C1G

P6:G|≡S⇒S↔ C1G

P7:S|≡S↔ C1G

P8:G|≡S↔ C2G

1 We get S|# S1G, S2G, and Gid from P1.

2 We get S(SC1G, SCG, Gid)SEp, EcG from message 2.

3 We can get S|G(SC1G, SC2G, Gid) by using the knowledge from the previous phase and applying P3 and R3.

4 We may obtain S|G(SC1G, SC2G, Gid) by combining steps 1, 3, and R2.

5 We can produce S|GSC1, C2G by using the preceding process and taking into account the security goal2, so accomplishing the desired security aim.

6 Step 5 can be applied to get S|GSC2G.

7 The application of step 6 results in the production of S|SC2G.

8 We may acquire S|SC1, C2G and the desired Goal1 by using the preceding step 7, P1, Res5, and the security goal 2.

9 We may get G(SC1G, SC2G, Gid)SE,k EcG from message 3.

10 We may achieve GS(SC1G, SC2G, Gid) by making use of P4, R3, and the prior step.

11 The result is G|#(SC1G, SC2G, Gid), which we may get by combining P2 and R1.

12 G|S|(SC1G, SC2G, Gid) is attained using Steps 10, 11, and R2.

13 Goal 4 is effectively attained by adding R5 and making reference to the prior step, represented as G|S|S|C1, C2G.

14 The preceding step can be used to get G|S|S|C1G.

15 We may achieve G|SC2G by combining the preceding step, P6, and R4.

16 We accomplish the goal3, denoted by G|SC1, C2G, by combining the previous step with P8 and R5.

End

6.4 VALIDITY OF PROTOCOL EVALUATION

AVISPA was used to thoroughly validate the aforementioned protocols while CAS++ and HLPSL modelling methods were employed. In order to find any potential security holes, the processes were thoroughly analysed, paying close attention to pgoal3:G|SC1, C2G(end). According to the results of the simulation, the suggested protocol reliably prevents attacks and efficiently handles security issues in the VANET environment.

7. Conclusion and Potential Future Improvements

In this paper, we suggested a straightforward mutual authentication scheme for VANET that prioritises lightweight encryption methods, including the use of symmetric-key cryptography and the NCSH chaotic hash function. The protocol relies on two essential shared secret keys: the update key (Ec) for the communication session and the permanent key (Ek) for encrypting messages during the mutual authentication phase. These keys serve as the fundamental components on which the protocol depends. The operation of the protocol is fundamentally based on these keys. To ensure a safe connection between the sensor node and the RSU, the protocol incorporates a security mechanism in the mutual authentication portion. Our proposed strategy strikes a balance between performance and security, as shown by the security study performed using BAN-logic. The protocol functions as a reliable and secure mutual authentication method within VANET. Furthermore, the computation of transmission costs for each message sent supports its applicability for networks with constrained resources. This protocol can be used by VANET nodes and RSUs to save energy and money. Future work on the protocol's security will focus on investigating the use of bio-inspired meta-heuristic functions, which will add to the protocol's complexity and reinforce its security measures.

References

[1] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," Wireless Communications and Mobile Computing, vol. 202025 pages, Article ID 5129620, 2020

[2] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework," IEEE Transactions on Industry Applications, vol. 99, p. 1, 2020.

[3] S. M. Faisal and T. Zaidi, "Timestamp based detection of sybil attack in vanet," IJ Network Security, vol. 22, no. 3, pp. 397–408, 2020.

[4] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles," IEEE Access, vol. 8, pp. 43711–743724, 2020.

[5] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems," Computer Communications, vol. 153, pp. 527–537, 2020.

[6] Q. Zeng, Y. Tang, Z. Yu, and W. Xu, "A geographical routing protocol based on link connectivity analysis for urban VANETs," Journal of Internet Technology, vol. 21, no. 1, pp. 41–49, 2020.

[7] M. Sohail, R. Ali, M. Kashif et al., "Trustwalker: an efficient trust assessment in vehicular internet of things (viot) with security consideration," Sensors, vol. 20, no. 14, Article ID 3945, 2020

[8] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: communication, applications and challenges," Vehicular Communications, vol. 19, Article ID 100179, 2019.

[9] Z. Afzal and M. Kumar, "Security of vehicular ad-hoc networks (vanet): a survey," Journal of Physics: Conference Series, vol. 1427, no. 1, Article ID 012015, 2020.

[10] A. Awang, K. Husain, N. Kamel, and S. Aissa, "Routing in vehicular ad-hoc networks: a Survey on single- and cross-layer design techniques, and perspectives," IEEE Access, vol. 5, pp. 9497–9517, 2017.

[11] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in vanet," IET Information Security, vol. 14, no. 1, pp. 99–110, 2019.

[12] Z. A. Abdulkader, A. Abdullah, M. Taufik Abdullah, and Z. Ahmad Zukarnain, "Vehicular ad hoc networks and security issues: survey," Modern Applied Science, vol. 11, no. 5, Article ID 30, 2017.

[13] A. Kumar and M. Bansal, "A review on vanet security attacks and their countermeasure," in Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 580–585, IEEE, Solan, India, September 2017.

[14] S. Hussain and S. A. Chaudhry, ""Comments on "biometricsbased privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment"" IEEE Internet of 9ings Journal, vol. 6, no. 6, pp. 10 936–10 940, 2019.

[15] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study," International Journal of Security and Its Applications, vol. 10, no. 5, pp. 261–274, 2016.

[16] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, "Vanet security and privacy-an overview," International Journal of Network Security & Its Applications, vol. 10, no. 2, pp. 13–34, 2018.

[17] A. Suman and C. Kumar, “A behavioral study of sybil attack on vehicular network,” in Proceedings of the 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), pp. 56–60, IEEE, Dhanbad, India, March 2016.

[18] A. N. Upadhyaya and J. Shah, “Attacks on vanet security,” International Journal of Computer Engineering and Software Technology, vol. 9, no. 1, pp. 8–19, 2018.

[19] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, “An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure,” International Journal of Communication Systems, vol. 32, no. 16, Article ID e4137, 2019.

[20] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, “A novel mechanism of detection of denial of service attack (dos) in vanet using malicious and irrelevant packet detection algorithm (mipda),” in Proceedings of the International Conference on Computing, Communication & Automation, pp. 414–419, IEEE, Noida, India, May 2015.

[21] Vaqur, M. ., Kumar, R. ., Singh, R. ., Umang, U., Gehlot, A. ., Vaseem Akram, S. ., & Joshi, K. . (2023). Role of Digitalization in Election Voting Through Industry 4.0 Enabling Technologies. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 123–130. https://doi.org/10.17762/ijritcc.v11i2.6136

[22] T. Zaidi and S. Faisal, “An overview: various attacks in vanet,” in Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), pp. 1–6, IEEE, Greater Noida, India, December 2018.

[23] H. El Hadj Kalil, A. D. Kora and S. Boumerdassi, "Security in VANETs: Lightweight Protocol for Group-of-Vehicles Masters (LPGVM)," 2020 22nd International Conference on Advanced Communication Technology (ICACT), 2020, pp. 6-11, doi: 10.23919/ICACT48636.2020.9061225.

[24] Z. Wei, J. Li, X. Wang and C. -Z. Gao, "A Lightweight Privacy-Preserving Protocol for VANETs Based on Secure Outsourcing Computing," in IEEE Access, vol. 7, pp. 62785-62793, 2019, doi: 10.1109/ACCESS.2019.2915794.

[25] S. Son, J. Lee, Y. Park, Y. Park and A. K. Das, "Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 3, pp. 1346-1358, 1 May-June 2022, doi: 10.1109/TNSE.2022.3142287.

[26] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar and N. Kumar, "A Lightweight Privacy-Preserving Authentication Protocol for VANETs," in IEEE Systems Journal, vol. 14, no. 3, pp. 3547-3557, Sept. 2020, doi: 10.1109/JSYST.2020.2991168.

[27] A. Mansour, K. M. Malik, A. Alkaff and H. Kanaan, "ALMS: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1663-1678, March 2021, doi: 10.1109/TITS.2020.2975226.

[28] R. I. Abdelfatah, N. M. Abdal-Ghafour and M. E. Nasr, "Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions," in IEEE Access, vol. 10, pp. 1096-1115, 2022, doi: 10.1109/ACCESS.2021.3137877.

[29] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar and M. A. Saleem, "Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF," in IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 12158-12167, Nov. 2021, doi: 10.1109/TVT.2021.3118892.

[30] Pathak, D. G. ., Angurala, D. M. ., & Bala, D. M. . (2020). Nervous System Based Gliomas Detection Based on Deep Learning Architecture in Segmentation. Research Journal of Computer Systems and Engineering, 1(2), 01:06. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/3

[31] W. Othman, M. Fuyou, K. Xue and A. Hawbani, "Physically Secure Lightweight and Privacy-Preserving Message Authentication Protocol for VANET in Smart City," in IEEE Transactions on Vehicular Technology, vol. 70, no. 12, pp. 12902-12917, Dec. 2021, doi: 10.1109/TVT.2021.3121449.

[32] J. Zhou, Z. Cao, Z. Qin, X. Dong and K. Ren, "LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 420-434, 2020, doi: 10.1109/TIFS.2019.2923156.

[33] S. Lv and Y. Liu, "PLVA: Privacy-Preserving and Lightweight V2I Authentication Protocol," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6633-6639, July 2022, doi: 10.1109/TITS.2021.3059638.

[34] J. Zhang and Q. Zhang, "On the Security of a Lightweight Conditional Privacy-Preserving Authentication in VANETs," in IEEE Transactions on Information Forensics and Security, doi: 10.1109/TIFS.2021.3066277.

[35] G Bindu, R .A Karthika, “Design of High Secured Multi Scroll Attractor Based Henon Map Chaotic Encryption Scheme for VANET Communication,” Journal Engineering Research, pp. 1-16, 2021, https://doi.org/10.36909/jer.ICETET.14973.

[36] Adhikary, K., Bhushan, S., Kumar, S. et al. Hybrid Algorithm to Detect DDoS Attacks in VANETs. Wireless Pers Commun 114, 3613–3634 (2020). https://doi.org/10.1007/s11277-020-07549-y