Scauthenticate: Efficient and secure certificateless aggregate signature based authentication scheme for vehicular ad-hoc networks

[1]**C.RAJKUMAR**, Ph.D Research Scholar, Department of Computer Science, Kongu Arts and Science College, Erode

[2]**Dr.T.A.SANGEETHA**, Associate Professor, Head and Department of Computer Applications, Kongu Arts and Science College, Erode

[3]**C.RAJKUMAR**, Assistant Professor, Department of Computer Applications
Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore

Abstract

With the use of IoT technology, the Vehicular Ad-hoc Network (VANET) facilitates encrypted communication between vehicles to enhance road safety and traffic management. When it comes to the safety of communications between vehicles in a VANET or between vehicles and infrastructure, vehicle access control authentication is a crucial safety function. Also, original versions of all correspondence must be made available. Meanwhile, safeguards are needed to prevent the inappropriate disclosure of personal information and other forms of intrusion in autos. In addition, VANETs have difficulties such restricted bandwidth, high mobility, and scalability. In this work, we proposed SCAuthenticate as certificate-free authentication technique based on digital signatures that may be used in VANETs. Our method eliminates the need for sophisticated certificate administration, a problem plaguing public key infrastructures, and the key escrow problem, which affects identity-based frameworks. In addition, the Road Side Unit (RSU) saves time and space by using aggregate signatures instead of validating and keeping individual signatures on multiple messages from various cars. The proposed method utilized the MECDA and map to point algorithm. By using our strategy, malicious vehicles will no longer be able to undermine the security of VANETs. As a result, the proposed method significantly reduces the need for computational resources. Security and performance benchmarks reveal that our solution is superior to state-of-the-art alternatives.

Keywords: Authentication, Certificate less, MECDA, VANET, ScAuthenticate, Signature.

DOI: 10.48047/ecb/2023.12.si4.985

I INTRODUCTION

In the last several years, fifth-generation (5G) networks have been a prominent issue because of the fast expansion of communication technology [1]. In addition, 5G networks enable the interconnection of everything while achieving high-speed data transfer [2]. The Internet of Vehicles (IoV) is a foundational use case for 5G networks because of the speed with which data can be transmitted between automobiles, RSUs (roadside units), data centers, and mobile devices. In contrast to traditional VANETs, IoV can evaluate data from a wide variety of sensors and other vehicles in real time to provide intelligent driving assistance [3-7]. Congestion and accidents can be reduced, resulting in less time spent in transit and less environmental impact. While there are advantages to using IoV, there are also some obstacles that prevent it from being widely used. The invasion of personal space is one problem. A hostile opponent may acquire information about cars, such as routes and status, without adequate privacy protection to conduct an attack. Fortunately, the use of pseudonyms in conversations helps circumvent this issue. Then, the vehicles may interact with each other or with RSUs using the pseudonym [8-12].

VANETS has many advantages, but security and privacy issues arise when cars share information. An attacker in a VANET can simply broadcast false information to RSUs and other automobiles due to the open nature of the wireless network, which can cause traffic jams. Communicate truthfully and reliably to ensure the safety of all road users. Possible message security with cutting-edge cryptographic algorithms[13-17]. As a result, we need to deal with issues like message integrity, source authentication, traceability, and unlinking in VANET-based V2I interactions. In VANETs, digital signature-based authentication mechanisms have been developed in PKI-based, ID-based, and Certificateless-based cryptographic frameworks. Because certain entities in VANETs (such as RSUs and OBUs) have limited computing and storage capabilities, we must consider system efficiency while developing a practical authentication solution for effective communication in VANETs [19].

Integration of new and established technologies with IoT systems has a positive effect on the Fourth Industrial Revolution. The IoT might cause a major shift in the way many businesses operate. Health care, urban design, energy, intelligent transportation, and more all fall within this category. The main contribution of the paper is MECDA and map-to-point algorithm.

The rest of this article is organized as follows. Section II presents related work in VANETs as signature aggregate schemes. Section III introduces the Sc-authenticate model and algorithm details. Simulation results analysis and performance valuation are provided in Section IV. Finally, Section V concludes this paper and discusses future work.

II BACKGROUND STUDY

Cui, J et al. (2018) [3] to facilitate secure vehicle-to-infrastructure (V2I) connections in VANETs, a certificate less aggregate signature that does not rely on pairings was developed. The proposed system meets all of the VANET security standards, as determined by the findings of the security study. The given signature scheme does not make use of MapToPoint or any other pairing operations. The authors of this work should stress that the idea is most useful when a number of vehicles are located within the range of a single RSU or application server.

Hashimoto, K., & Ogata, W. (2019) [5] the authors proposed the first comprehensive but concise Constant-size, aggregated CAS signatures are used in a certificate-less aggregate signature (CAS) CLAS system. The author here shows that his technique benefits from unlimited aggregation. Due to the need for individually distinct state information for each signature in conventional compact systems, it is not possible to combine signatures from the same user.

Kamil, I. A., & Ogundoyin, S. O. (2019) [6] for vehicular ad hoc networks, the authors presented a novel certificate less aggregate signing technique based on Elliptic Curve Cryptography. These authors developed a batch verification approach to speed up and enhance the efficiency of signature validation by requiring the verifier to do just two scalar multiplication operations, regardless of the number of signatures being confirmed.

Kumar, P., & Sharma, V. (2017) [8] the authors of A certificate less aggregate signature CLAS presented a cryptanalysis showing that their method had weaknesses against type-2 attackers KGC acts as a bad guy with access to some of the user's private key in a type-2 adversarial scenario. Following this, the authors updated their CLAS approach to place greater focus on plugging security holes in the victim's scheme.

Malhi et al. (2019) [11] the author have compared and analyzed the various attacks and prospective adversaries, and provided analysis and recommendations for countermeasures Various forms of cryptography, including public-key and symmetric-key systems, as well as identity-based and certificate-free cryptography, are discussed. The author took a look at how things stand now in terms of cryptographic security and trust-based models. A comprehensive comparison study of the proposed security techniques in light of the used strategy was also provided. We then compared the features of these systems to those of vehicular ad hoc networks (VANETs) and summed up the most important open questions in the industry.

Ogundoyin, S. O., & Kamil, I. A. (2021) [13] Using a neuro-fuzzy algorithm, the authors boost VANET performance and make the system more resistant to DoS assaults. This author utilised two Merkle Tree Structure-based block chains to facilitate fast and transparent revocations. With the goal of reducing the computational load on a roadside unit (RSU) in a heavy traffic situation, a batch verification approach was created to certify the presence of vehicles entering the RSU's network coverage in a large number.

Ren Y et al. (2021) [15] presents a robust certificate-less signing mechanism that permits VANET connection to be authenticated while yet protecting users' privacy. Author's method reduces reliance on bilinear pairings, which in turn reduces the computational burden of verifying message signatures in a mobile unit (RSU).

X. Hu et al. (2020) [17] First, they conduct a safety analysis of the certificate less aggregate signature CLAS method they propose. Two attacks are detailed in the study that shows how an attacker can forge an aggregate signature using this CL-AS system, proving that the method is insecure. Finally, the authors provide a more effective CL-AS framework. The updated method not only addresses the previous security hole, but it also retains nearly all of the effectiveness of the original. There is no need for expensive bilinear pair operations in this system, therefore the computation required is quite low. It has potential applications in a number of fields, including ad hoc, sensor, and vehicle networks.

Zhao et al. (2019) [19] these authors introduced an original tactic that can repel both A1 and A2 attacks. In this case, the random oracle model has been used to verify the author's solution is safe. Extensive simulation results demonstrate that the author's approach far outperforms the state of the art. It was clear that this author's approach was better suited to a low-bandwidth context due to its high computational cost, inefficient communication, and lack of security measures.

III PROPOSED METHODOLOGY

3.1 Network Model

An intelligent vehicle as conceived in effectively contains a series of sensors (face radar, reverse radar, etc.) that receive valuable information about the environment, which is not usually perceived by the driver alone.

3.2 Road Side Unit:

The roadside machine is a computer that is attached next to or at a certain spot, for example, parking or intersection.

3.3 Sc-authenticate model

The Proposed model is generated using Modified Elliptic Curve Digital signature algorithm with map-to-point algorithm.

3.4 Modified Elliptic Curve Digital Signature Algorithm

1. The field order q.
2. A a representation indication for the field elements of Fq, denoted by the FR field.
3. Seed S if the elliptic curve was generated at random.
4. Elliptic curve E over Fq has an equation of the form y2 = x3 + an x + b (for a prime field) or y2 + xy = x3 + an x2 + b (for a binary field). These coefficients, a, b, are defined as functions of the field Fq.
5. A finite point P in affine coordinates is defined by two field elements xp and yp in Fq, as P = (xp; yp) 2 E. (Fq). The fundamental point, or P.
6. P's n-th order.
7. Cofactor h = #E(Fq)=n:

The cryptographic hash function H is denoted by the letter H, and it produces hashes with a maximum bit length of n. It is OK to cut off H's outputs if this condition is not satisfied.

3.4.1 MECDSA Signature generation

The inputs are the private key d, the message m, and the domain parameters D = (q; FR; S; a; b; P; n; h).

```
Begin
$select\ k \in_R [1, n-1]$;
Convert x1 to an integer and use it in the formula kP=(x 1,y 1);
The formula for r is: x1 minus n mod r;
Then, if r = 0,
to the first stage
end
find e = H (m);
compute $s = k^{-1}(e + dr)$mod n;
```

```
when s = 0
continue to Method 1
end
return (r,s);
end
```

3.4.2 ECDSA signature Verification

```
Input: Domain (D) = (q,FR,S,a,b,P,n,h), Message (m), and Signature (S) = (Q,FR,S) (r,s).
Output : This signature is either accepted or rejected.
begin
Please ensure that both r and s are integers and fall inside the range [1; n1]. In the event that verification is unsuccessful,
return (Reject the signature) ;
Input e = H into your calculator (m) ;
To get w, divide s1 by n;
 can solve for u1 = ew mod n and u2 = wr mod n by using the following formulas;
Find X = u1P + u2Q:
then (if X = O)
return (Reject the signature)
end
Extract the integer value _x1 from the X coordinate x1;
In other words, v = _x1 mod n. ;
if (and only if) v equals (and is proportional to) r
end
```

3.4.3 Two Key ECDSA Signature Generation

```
Inputs consist of the message m, the private keys d1 and d2, and the domain parameters D = (q, FR, S, a, b, P1R, n, h).
Signature (x1, s1; s2) start
1 Select k1 and k2 2R [1; n 1];
2 Figure out that k1+P1+k2=S (x1; y1);
3 Assuming S=O,
goto step 1
end
4 Compute $e = H(m)$.;
5 Convert the element of the field x1 to an integer. (often represented as a 1 in a vector) ;
6 Determine $s1 = e k1 + x d1$ and $s2 = e k2 + x d2$;
7 return (x1, s1; s2);
End
```

3.5 Design of Proposed map-to-point-Hash Function

Each hash function is made up of two parts: a compression function and a construction function. The technique for continually calling the compression function to process a variable-length message is the construction, and the compression function is the mapping function that lowers a larger arbitrary-size input to a smaller fixed-size output. Hash functions are often made without a secret ingredient. However, many modern, successful attacks have been constructed against these standard, commonly used hash algorithms (SHA-1, MD5, etc.). As was said before, it is necessary to demonstrate the safety of an algorithm, although the vast majority of newly developed algorithms are really variants of existing, proven ones. There will be more built-in safety elements in the new design if the old one has few. As with MD5, this method relies on its familiar structure for its security. The suggested approach is also more secure than MD5 against many of the known attacks since the key is included into each round of operation on individual blocks.

Existing hashing algorithms may be enhanced by increasing the number of rounds of operations rather than the mandated number of fundamental functions (using more than four primitive functions in the case of MD5, for instance) or by adding additional sophisticated coding or permutation phases (for example, using more scrambling techniques in SHA-1). Alternatively, total buffer space can be increased and a different mixi function can be used. The most popular method for creating hash functions is based on block cyphers. Hash functions use this tactic by using a compression function analogous to a block-cipher that takes in two parameters, a message block and a key, to compress the message. These days, if an attack on a protocol takes more than 2128 steps, we may consider it secure. Nonetheless, more safety measures will be essential in the not-too-distant future.

The Key Distribution Center (KDC) is in charge of sending the conversation's shared session key to both parties. KDC does this using the master keys of both parties. Since no one else on the network has access to either of their private keys, no one else can read the original conversation or use the session key. Only KDC and the two parties involved in the message delivery process know the shared secret key. Since the sender and the receiver share the same key, this method may help verify the sender's identity.

Both the hash compression function and the keyed encryption technique are included into this strategy. As an input to the keyed operation is the result of the compression algorithm for each block. The compression function produces a 128-bit long output. Additionally, the keyed function takes in a 64-bit chunk of data at a time. As a result, the result of the compression function is split into two equal-sized 64-bit blocks and then processed twice. Both 64-bit blocks are then subjected to the keyed function (encryption function) in turn. In all, the output consists of 128 bits, or 64 bits for each of the left and right channels. This 128-bit output is converted into a 128-bit CVq for use in the upcoming input block's compression function processing.

The proposed algorithm described as given pseudo code:

```
Step 1: Start
Step 2: Put padding bits at the end of input message
Step 3: Put length of original message at the output of Step 2.
Step 4: Divide the output of Step 3 into L blocks of equal size. (512 bit blocks).
Step 5: Initialize 128 bit MD buffer
Step 6: Repeat Steps 7 to 11 for all 512 bit L blocks
Step 7: Calculate 128 bit hash value for the ith block
Step 8: Break output of Step 7 into two equal size blocks (64 bits each).
Step 9: Encrypt both blocks (outputs of Step7) using keyed block encryption function.
Step 10: Combine both 64 bit outputs calculated in Step 9.
Step 11: Use the output of Step 10 as CV for next 512 bit block.
Step 12: Transmit the final output of hashing of last block ($L^{th}$ block) as final hash value to the receiver.
Step 13: End
```

Following figure 1 depicts the overall processing as per this scheme

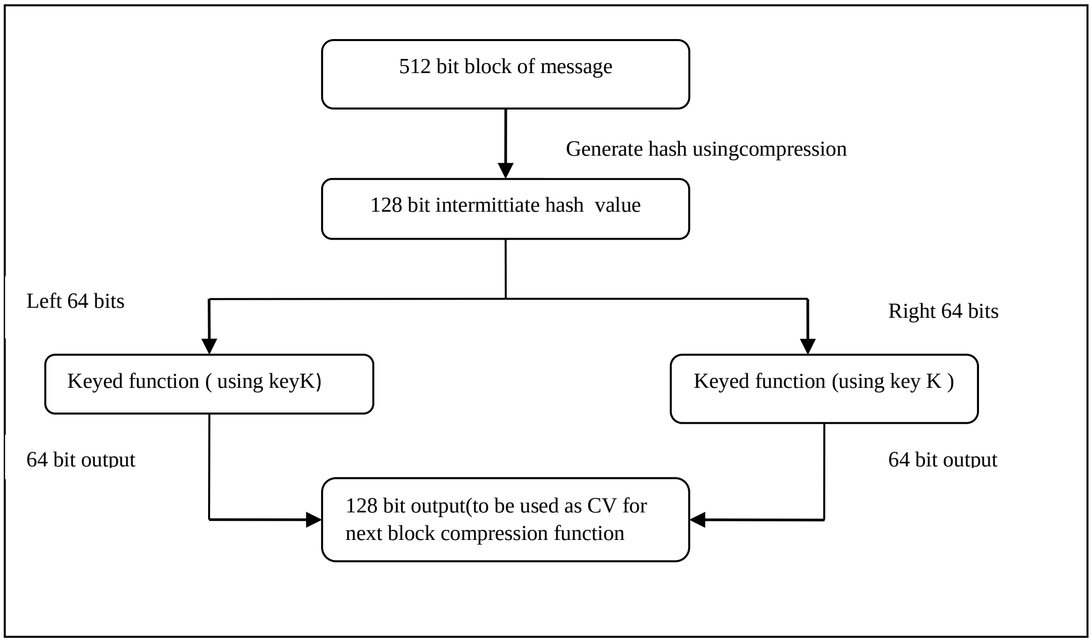
512 bit block of message
Generate hash usingcompression
128 bit intermittiate hash value
Left 64 bits
Right 64 bits
Keyed function (using keyK)
Keyed function (using key K)
64 bit output
64 bit output
128 bit output(to be used as CV for next block compression function

Figure 1 : Use of keyed function in construction hash using compression function

IV RESULT AND DISCUSSION

We simulate our proposed protocol in NS2 Simulator. We compare our Sc-authenticate Model with the cross-layer approach and Multi-factor secured and privacy with VANET (MFSPV) and Lightweight Privacy-preserving Authentication (LPPA). The Network size is 550 x 480 m. and the network parameters as communication overhead, signature generation, verification and delay.

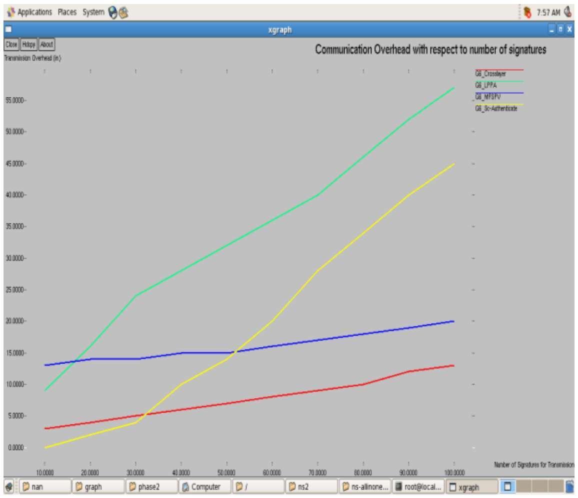

Figure 2: Communication overhead with respect to number of signatures

The network model has aggregate the signature with respect to the number of signatures is compared with LPPA, MFSPV, Cross layer and SCAuthenticate method represented in figure 2. X-axis denotes the number of signatures for transmission and Y-axis denotes the Transmission overhead.

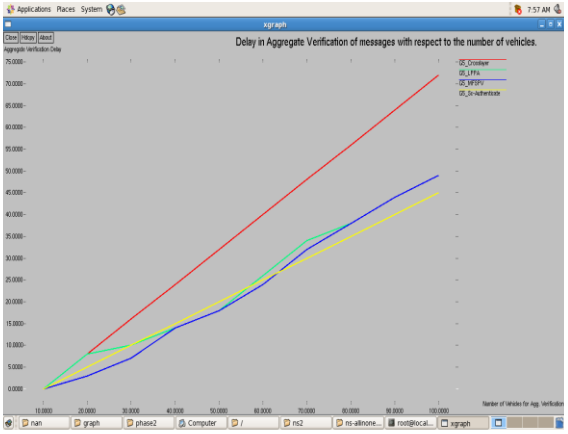

Figure 3: Comparison chart for Delay aggregate verification of messages with respect to the number of vehicles

Delay aggregate verification of messages with respect to the number of vehicles is compared with LPPA, MFSPV, Cross layer and SCAuthenticate method represented in figure 3. X-axis denotes the number of vehicles for aggregate verification and Y-axis denotes the aggregate verification delay.

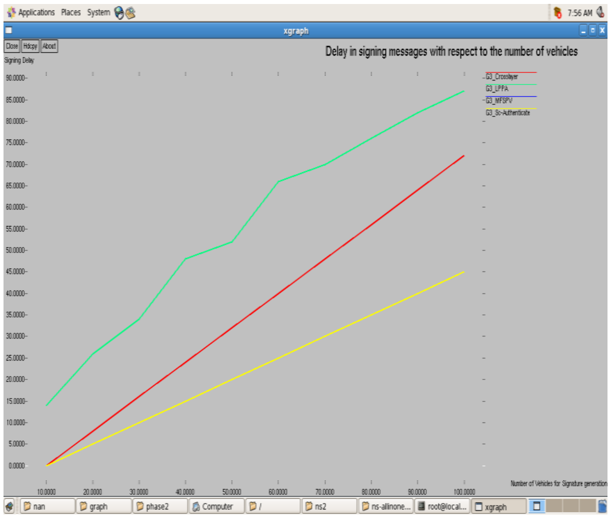

Figure 4: Comparison chart for Delay in signing messages with respect to the number of vehicles

Delay in signing messages with respect to the number of vehicles is compared with LPPA, MFSPV, Cross layer and SCAuthenticate method represented in figure 4. X-axis denotes the number of vehicles for signature generation and Y-axis denotes the signing delay.

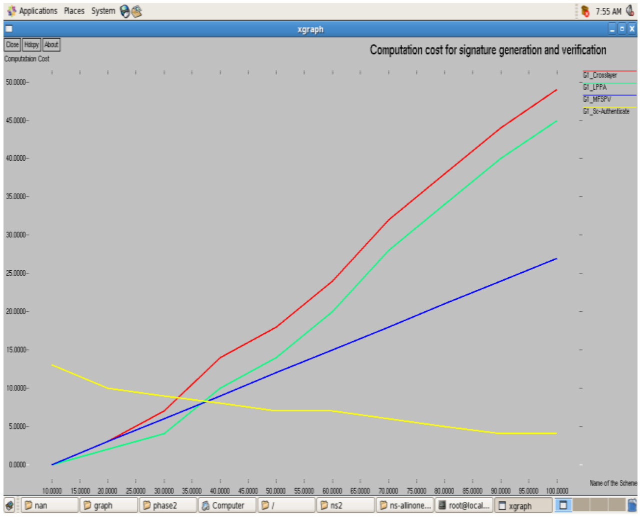

Figure 5: Comparison chart for computation cost for signature generation and verification

Computation cost for signature generation and verification is compared with LPPA, MFSPV, Cross layer and SCAuthenticate method represented in figure 5. X-axis denotes the number of vehicles and Y-axis denotes the Computation cost.

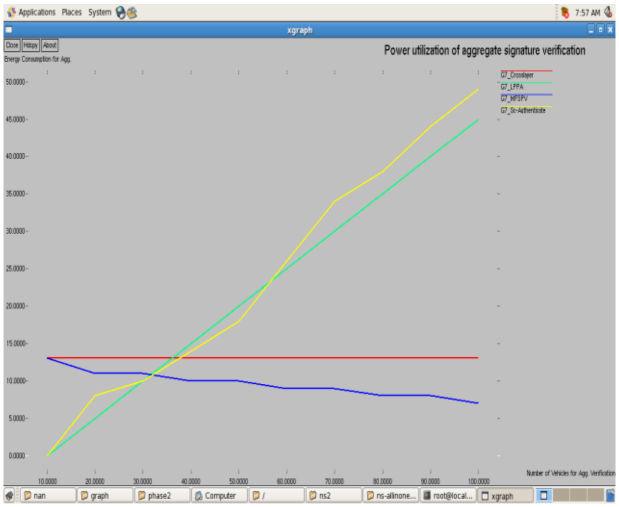

Figure 6: Comparison chart for Power utilization of aggregate signature verification

Power utilization of aggregate signature verification is compared with LPPA, MFSPV, Cross layer and SCAuthenticate method represented in figure 6. X-axis denotes the number of vehicles for aggregate verification and Y-axis denotes the Energy computation.

V CONCLUSION

This study reveals a reliable and fast authentication method based on ScAuthenticate for VANETs. Neither certificate management nor key escrow are problematic in the proposed system. Using the proposed technology, a single signature may be used to authenticate a wide range of messages sent by a variety of vehicles. The suggested aggregation method reduces verification time, calculation cost, bandwidth need, and RSU storage space. Existing Cross layer, LPPA and MFSPV methods are compared with proposed VANET authentication solutions are much more computationally intensive than the pairing-free method proposed. As a result, the suggested remedy has the potential to prevent malevolent vehicles from endangering VANET security. In a comprehensive evaluation of performance, the SCAuthenticate authentication technique was found to be the best in terms of security, computing, and communication. For further, to focus on data transmission security with path management.

VI REFERENCES

[1]. Ali, I., Hassan, A., & Li, F. (2019). Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. Vehicular Communications. doi:10.1016/j.vehcom.2019.02.002

[2]. Chen, Y.-C., Tso, R., Mambo, M., Huang, K., & Horng, G. (2014). Certificateless aggregate signature with efficient verification. Security and Communication Networks, 8(13), 2232–2243. doi:10.1002/sec.1166

[3]. Cui, J., Zhang, J., Zhong, H., Shi, R., & Xu, Y. (2018). An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks. Information Sciences, 451-452, 1–15. doi:10.1016/j.ins.2018.03.060

[4]. G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, D. V. R. K. Reddy and M. Padmavathamma, "Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1908-1920, 1 Feb.1, 2021, doi: 10.1109/JIOT.2020.3019304.

[5]. Hashimoto, K., & Ogata, W. (2019). Unrestricted and compact certificateless aggregate signature scheme. Information Sciences, 487, 97–114. doi:10.1016/j.ins.2019.03.005

[6]. Kamil, I. A., & Ogundoyin, S. O. (2019). An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. Journal of Information Security and Applications, 44, 184–200. doi:10.1016/j.jisa.2018.12.004

[7]. Kar, J., Liu, X., & Li, F. (2021). CL-ASS: An efficient and low-cost certificateless aggregate signature scheme for wireless sensor networks. Journal of Information Security and Applications, 61, 102905. doi:10.1016/j.jisa.2021.102905

[8]. Kumar, P., & Sharma, V. (2017). On the Security of Certificateless Aggregate Signature Scheme in Vehicular Ad Hoc Networks. Soft Computing: Theories and Applications, 715–722. doi:10.1007/978-981-10-5687-1_63

[9]. L. Deng, B. Ning and Y. Jiang, "A Lightweight Certificateless Aggregation Signature Scheme With Provably Security in the Standard Model," in IEEE Systems Journal, vol. 14, no. 3, pp. 4242-4251, Sept. 2020, doi: 10.1109/JSYST.2020.2970427.

[10]. Lai, H. Li, R. Lu, R. Jiang and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," 2014 IEEE International Conference on Communications (ICC), 2014, pp. 1011-1016, doi: 10.1109/ICC.2014.6883452.

[11]. Malhi, A. K., Batra, S., & Pannu, H. S. (2019). Security of Vehicular Ad-hoc Networks: A Comprehensive Survey. Computers & Security, 101664. doi:10.1016/j.cose.2019.101664

[12]. N. B. Gayathri, G. Thumbur, P. Rajesh Kumar, M. Z. U. Rahman, P. V. Reddy and A. Lay-Ekuakille, "Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9064-9075, Oct. 2019, doi: 10.1109/JIOT.2019.2927089.

[13]. Ogundoyin, S. O., & Kamil, I. A. (2021). An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. Vehicular Communications, 31, 100384. doi:10.1016/j.vehcom.2021.100384

[14]. P. Kumar, V. Sharma and G. Sharma, "Certificateless aggregate signature schemes: A review," 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 531-536, doi: 10.1109/CCAA.2016.7813777.

[15]. Ren, Y., Li, X., Sun, S.-F., Yuan, X., & Zhang, X. (2021). Privacy-preserving batch verification signature scheme based on blockchain for Vehicular Ad-Hoc Networks. Journal of Information Security and Applications, 58, 102698. doi:10.1016/j.jisa.2020.102698

[16]. Wasef and X. Shen, "ASIC: Aggregate Signatures and Certificates Verification Scheme for Vehicular Networks," GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, 2009, pp. 1-6, doi: 10.1109/GLOCOM.2009.5425238.

[17]. X. Hu, W. Tan, C. Ma, F. Chen and C. Yu, "Study on Security Analysis and Efficient Imrovement of Certificateless Aggregate Signature Scheme," 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), 2020, pp. 343-346, doi: 10.1109/ICSESS49938.2020.9237675.

[18]. Y. Liang and Y. Liu, "Analysis and Improvement of an Efficient Certificateless Aggregate Signature With Conditional Privacy Preservation in VANETs," in IEEE Systems Journal, 2022, doi: 10.1109/JSYST.2022.3180221.

[19]. Zhao, Y., Hou, Y., Wang, L., Kumari, S., Khan, M. K., & Xiong, H. (2019). An efficient certificateless aggregate signature scheme for the Internet of Vehicles. Transactions on Emerging Telecommunications Technologies. doi:10.1002/ett.3708