NVEO
Natural Volatiles & Essential Oils

CSBA: Secure Certificateless Aggregate Signature-Based Authentication Scheme For Vehicular Ad-Hoc Networks

N. Parthiban, Ph.D[1]., Dr. G. Dheepa[2]

[1]Research Scholar, P.K.R Arts College for Women, Gobichettipalayam, Erode, Tamilnadu
[2]Associate Professor, P.K.R Arts College for Women, Gobichettipalayam, Erode, Tamilnadu

Abstract

A rising number of vehicle applications need heightened security measures. A typical form of authentication for VANETs (Vehicular Ad Hoc Networks) is the use of a group signature. Due to the dynamic nature of wireless networks, there are several hurdles to peer-to-peer communications. For VANETs (vehicle-to-vehicle communication networks), CSBA stands for secure certificateless aggregate signature-based authentication. They choose their RSU based on factors that determine the generation of a Partial private key pair. All vehicles have an OBU that is tamper-resistant and can generate PPK pairs and self-certify PPK generated using the Signature generation procedure. It is necessary for every vehicle that joins the group to authenticate itself to the leader to accomplish certificateless aggregation. It then sends traffic-related messages through the group key to the group leader, who verifies the messages and broadcasts them in a single hop to reduce the computational burden on each vehicle's message verification system. The CSBA approach is also used to protect user privacy by preventing an attacker from linking a message to the transmitted vehicle. The extensive research, simulations, and vehicle-to-vehicle communication are performed in the best way.

Keywords: VANET, PPK, CSBA, Signature Generation, Certificateless aggregate

1 INTRODUCTION

In recent years, the VANET has become more popular. Roadside units (RSUs) and fast-moving vehicles are the most common components of VANETs. In addition to communicating and storing essential data, each vehicle is equipped with an onboard unit (OBU). Periodic safety signals known as beacons are the primary means VANET components communicate with one another. A source vehicle should transmit a beacon message every 300–1000 milliseconds to keep neighbouring entities informed of their surroundings. These beacon messages provide information on the vehicle's speed, location, and heading direction [1].

Additionally, cars broadcast periodic alerts whenever they identify an occurrence such as traffic congestion or a pothole. Due to the complexity of the VANET, it is susceptible to a variety of security and privacy assaults [3]. When an attacker vehicle sends out fraudulent messages, it disrupts the VANET and is one of the most severe attacks recorded in the literature. Upon verification, the broadcaster of forged communications may deny involvement in their transmission, rendering the attacker impervious to discovery [4]. To combat these attacks, the RSU should verify the legitimacy of these communications. One the possibility of hundreds of vehicles running at any time, the verification procedure should be very efficient. RSU checks all vehicle communications in a timely way [8].

Numerous digital signature techniques have been suggested for VANET [9], [10]. A digital signature placed on communication ensures the message's originator's validity, integrity, and non-repudiation. [11] proposes a signature technique based on classical public-key cryptography (PKC). Their primary disadvantage is their significant certificate administration expense. There are proposals for group signature techniques that do not need certificates [12], [14]. Concerns with revocation, such as how to delete compromised and revoked signers without compromising the privacy of the signers themselves, are raised. These methods are more expensive to store and verify. IBC (identity-based cryptography) is another approach proposed, in which the vehicle's private keys are provided by a Trusted Authority [15, 16]. [15] (TA). A central authority holds all of a vehicle's private keys in an IBC-based system, which has key escrow problems.

Safety and traffic information, including weather conditions, broadcasting emergencies, route maps, and navigations, may be sent between cars through V2V or V2I communication [17]. These connections are carried over the same shared wireless network, which demands user privacy and data security containing critical information in safe driving settings.

The CSBA Scheme for VANETs is presented in this paper to overcome these challenges. The VANET system will be scalable and efficient due to our secure key distribution approach. Another method for securely transmitting keys from vehicles to nodes is using a shared symmetric key, which is much more efficient and has a low computational cost.

It's as follows in the rest of the article: Section II covers the existing literature review. A system model is described in Section III; Section IV lays out our preferred method of implementing the system. Section V provides an evaluation and analysis of our technique. Conclusions are drawn at the end of Section VI.

2 BACKGROUND STUDY

E. R. Agustina & A. R. Hakim [1] The authors use hierarchical pseudonyms and blind signatures to accomplish the security purpose. The authors demonstrate that this system protects users' privacy during authentication. Additionally, it is shown that this protocol acts as a deterrent against malicious conduct.

Celes, A. A., and Elizabeth, N. E. [2] begin by analyzing the propagation of erroneous information over networks. Then, detection algorithms are employed to identify nodes that utilize beacon signals to deceive their location. The simulation findings demonstrate that this sort of verification system efficiently identifies nodes distributing misleading information, thereby minimizing the propagation of false information regarding their location. While this strategy will not eliminate fraudulent attacks, it will significantly minimize erroneous position information.

V. Hemamalini et al. [5] Due to the inability to use dedicated channels in VANETs for concentrated data transmission, it is agreed that the throughput is sent efficiently with a minimal decrease in the given directing time, in an authenticated and certified manner. With the node vulnerable to helplessness and the connection's dynamic uptime, low-variability automobiles in an area are selected to exchange data with the lowest rate of misfortune/no misfortune factor in mind. To avoid unnecessary packet losses at the source, a shared key acceptance system that adapts to the topology of the directed route results in delayed RT upgrades. This work builds on the previous one by responding to out-of-range and guiding structures without affecting correspondence or uptime.

Tsai Jia-Lun [6] To undermine Biswas and Misic's security, this research suggests that public key leaking might be employed. The authors proposed a more secure authentication mechanism. An Elliptic Curve Digital Signature Algorithm method is used to build the system suggested in this article. Anti-repudiation is ensured by the suggested approach, which is resistant to assaults such as private key forgery and signature fabrication. Revocation and tracking capabilities are also shown in the suggested technique.

The authors of Liu, F., and Wang, Q. [7] Using the ring signature, we provide a batch verification method for VANETs. In contrast to earlier ring signature-based techniques, ring formation is limited to minimize the disruptions produced by hostile vehicles. A batch verification and bilinear pairing strategy keep costs down in most real-world applications where VANETs are present.

T. Matsukawa et al. [9] For the sake of speeding up the transmission, a new method of dynamically changing the number of verifications was proposed. Methods that validated all signatures and those that confirmed none were used to compare the received rate of the new methodology. Simulated findings show that the recommended technique boosted the received rate in a high vehicle density condition.

J. Shao et al. [11] The use of a novel group signature technique in conjunction with an effective threshold anonymous authentication system has been suggested. Using the threshold anonymous authentication protocol introduced in this paper, the decentralized group model and the threshold authentication technique may give threshold authentication, efficient revocations, unforgivably anonymity, and traceability in VANETs. For the record, the new group signature approach is the first to provide rapid message tracking and linkage.

Y. Xiaodong et al. [14] In VANETs, communications are protected using the trapdoor hash function and proxy signature. This system ensures verifiability, privacy, and traceability of the vehicle's identification. The research found that this technique dramatically decreases computing costs involved with signature verification and significantly enhances the real-time performance of communication messages.

C. Zhang et al. [17] Validation of safety signals received by cars is critical in VANETs. This method assures privacy while also ensuring speedy safety message authentication by merging batch group signature verification and GSK in a regional group architecture. This approach of group-signature-based authentication may meet security criteria while also outperforming other ways of group-signature-based authentication currently available.

3 SECURE CERTIFICATELESS KEY AGGREGATE

Network-coded communication with digital signatures has a source, a forwarder, and a sink on the VANET, as shown in Fig. 1. A signature verification key (SVK) may be used by all vehicles to verify the integrity of received data. The verification key is published by PPK Infrastructure. SVKs are assumed to be unique to each vehicle.

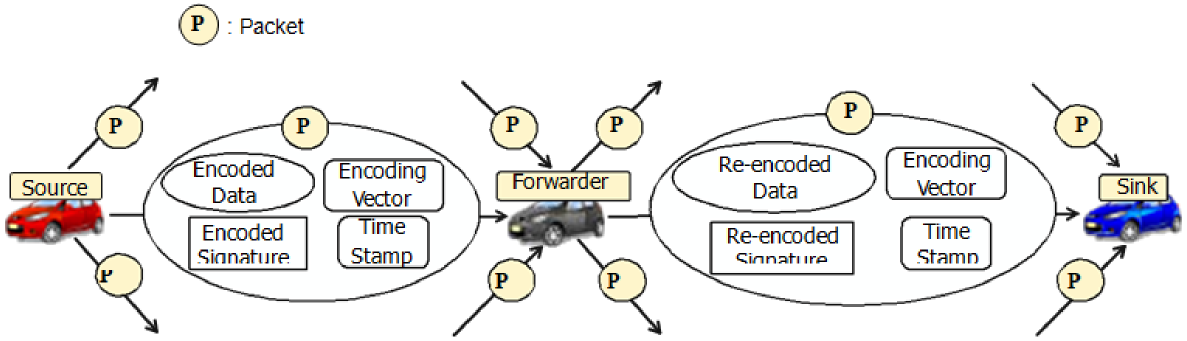

Figure 1: Communication Protocol

The Trusted Authority (TA) registers and certifies vehicles. The reliable backbone network links TA and RSUs securely. When an inquiry is necessary, TA may assist RSUs in determining the true identity of cars. The TA is the most secure component of the VANET design.

Road Side Units (RSUs): RSUs are the infrastructure created. RSUs are the building blocks of a domain. A domain's geographic location, infrastructure capacity, deployment strategy, and vehicle demographics may be used to estimate the number of RSUs in the domain.

Vehicular Nodes: Using the IEEE Standard 1609.2 radio, vehicles may connect and RSUs. [15] This is a wireless access standard for vehicle settings (WAVE). The group keys and their associated public and private key sets must be utilized for authentication and encryption/decryption for the cars to communicate. These keys are kept in a tamper-proof container [16].

C. Design Goals

Based on the system model and anticipated threats, this article seeks to fulfill the following security and performance goals.

Security Objectives:

Confidential or sensitive information, such as a person's name or address, should be secured when it is sent in the form of an authorized message.

RSU and mobile sensors must check each other to ensure that data collected from the source has not been tampered with while in route.

Mobile sensor IDs must be hidden throughout the authentication process to preserve the sender's private information.

Resilience of the Escrow: The user's private keys are not accessible to the key generating centre. As a result, even if KGC is hacked, the attacker will not obtain the user's private keys.

Performance objectives: The security approach should be as basic as feasible regarding transmission overhead and processing delay. Several signatures on a report should be verified before they are unsigned for a short period.

If one of the private keys of a mobile sensor is breached, the resulting data should not be available.

There are limits to mobile sensors and devices' power and storage capacity.

Consequently, the proposed method should be computationally sprightly.

CSBA: IMPLEMENTATION

Setup: This function receives a security parameter (k) and returns system parameters (params), a partial private key (s), and a master private key (P_{pub}) that corresponds to it. Execution and publication of parameters are then carried out following this method. The key is kept in a secure place.

PPK: A partial-private key (PPK) is possible when given the system parameters params and s and an ID_i for the entity in question, a partial-private key (PPK) is possible. A PPK D_i is the result. A secure channel sends the technique for creating D_i to the matched user *i*.

Key Gen: To generate a unique key for each user, each user must perform this function, which accepts the parameters and the user's identity ID_i as inputs. To get the PPK for the entity, it returns the secret value x_i.

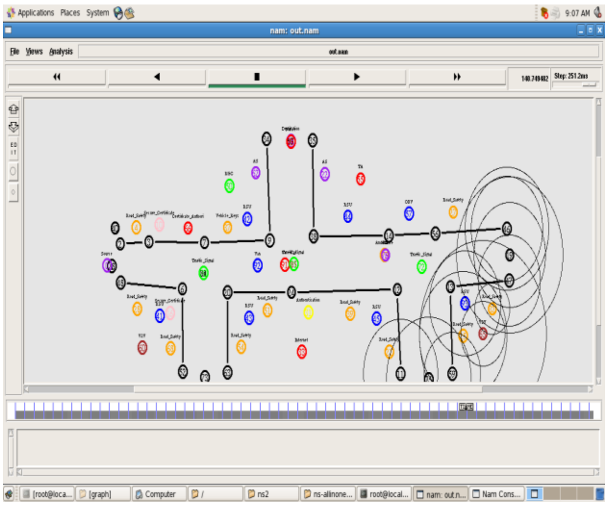

Figure 2: VANET simulation Environment

The Vehicles are authenticated secured with the environments using TA and RSU's, shown in figure 2.

Partial Private Key-Generation: *PPK* algorithm is interactively performed by the user ID*i* and KGC.

a) The user ID$_i$ arbitrarily chooses $x_i \in Z^*_q$ as the secret value and computes a PPK $Y_{ib} = x_iP$.

b) The user sends its identity and PPK (ID_i, Y_ib) to the KGC.

c) The KGC then randomly selects $yi \in Z^*_q$ and compute another PPK for the user $Y_{ia} = y_{iP}$, so the full Private key for the user is (Y_{ib}, Y_{ia}).

d) The KGC computes the PPK $D_i = y_i + s * Q_i$ where $Q_i = H_1(ID_i)$, and D_i is sent securely to the user ID$_i$.

e) The user ID$_i$ judges the validity of the PPK by checking $D_{iP} = Y_{ia} + P_{pub}H_1(ID_i)$.

Algorithm 2: Signature Generation

By using this signature generation technique, a safe method of establishing signatures among automobiles is built. As illustrated, the expressions are summarised in a structed manner.

Signature ID generation:

Step 1: $PID_v=T||E_p(ID_v)||HM||ID_{RSU}$ // vehicle v generates its pseudocode ID

V2R & R2V Communication

Step 2: RSU→*;<ID_{RSU}, TS, P, M_{ad}, none, SIG_{RSU} (ID_{RSU}||TS)>

Step 3: V_v→RSU; <ID_{RSU}, PID_v, TS, (PID_v||TS)>)

Step 4: RSU→*;<ID_{RSU}, TS, set_v(ALL), none (ID_{RSU}||TS)>)

V2V Communication

Step 5: V_v→V_w; <PID_v, TS, none, SIG(PID_v)||TS)>

Algorithm 3: Certificateless Key aggregate

Aggregate: One user's ID$_i$ and the PPK, Y_i and C_i on a message Mi are used as inputs for this procedure that is executed by the Certificateless Key aggregation signcryption generator. The message is ciphered with state information with the recipient's IDR and PPK Y_R matched. On messages $Min_{i=1}$, it generates an aggregated ciphertext *C*.

Aggregate-Verify: The recipient's identity Idf with accompanying PPK Y_R, state information, and the aggregated ciphertext C are all inputs to ID_R. If the aggregate signature verification succeeds, true is returned, otherwise false.

4 RESULTS AND DISCUSSION

The simulations are conducted using a VANET environment created using the Ns2 simulation tool, one TA, three RSUs, and 100 vehicle nodes travelling across a 900 x 600 operational space simulation area with a simulation period of around 512 seconds. Vehicles will move between positions at speeds ranging from 0 to 50 m/s. Communications between cars will be accomplished by transmitting packets at a data transfer rate of around 1MB.

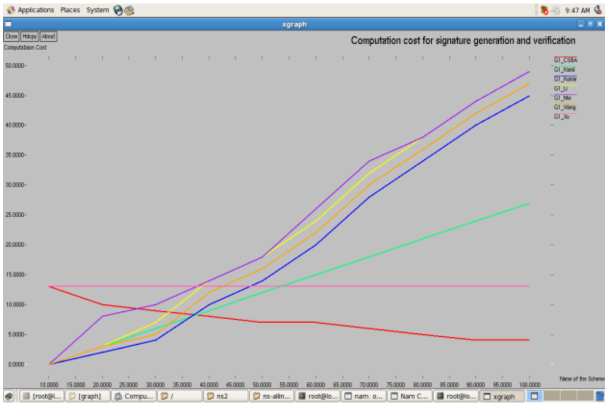

Figure 3: Computation cost for signature generation and verification

In comparison to other authors, the cost of computation for signature creation and verification is very cheap using the CSBA technique, as seen in Figure 3.

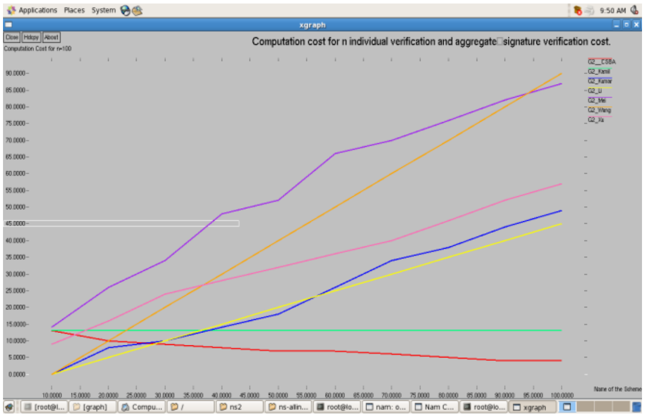

Figure 4: Computation cost for individual verification and aggregate signature verification cost

The comparison chart for the cost of computation for individual signature verification with the cost of aggregate signature verification is provided in Figure 4. The CSBA approach requires a minimal amount of computing.

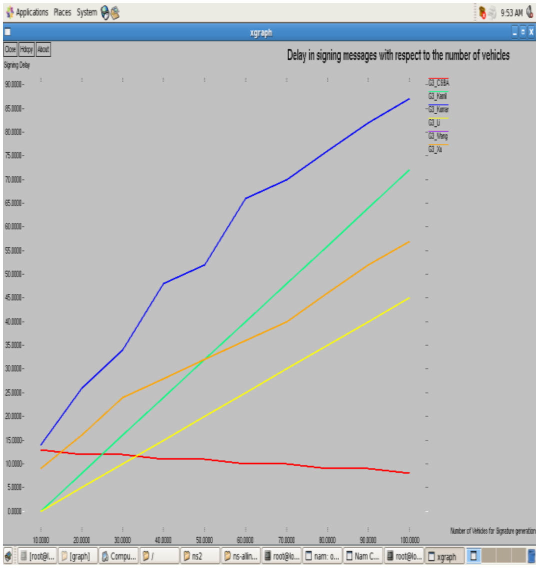

Figure 5: Delay in signing messages

Figure 5 illustrates a chart comparing the delay in signing messages pertaining to the number of cars. Numerous writers' suggested approaches have been compared to the CSBA method.

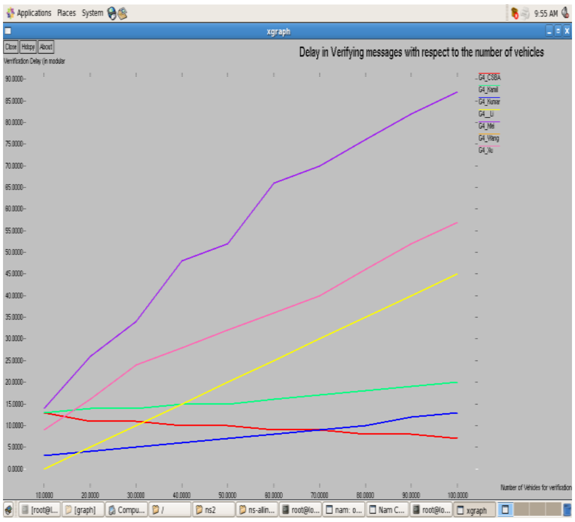

Figure 6: Delay in verifying messages

Figure 6 illustrates a comparison chart for the time required to validate communications about the number of cars.

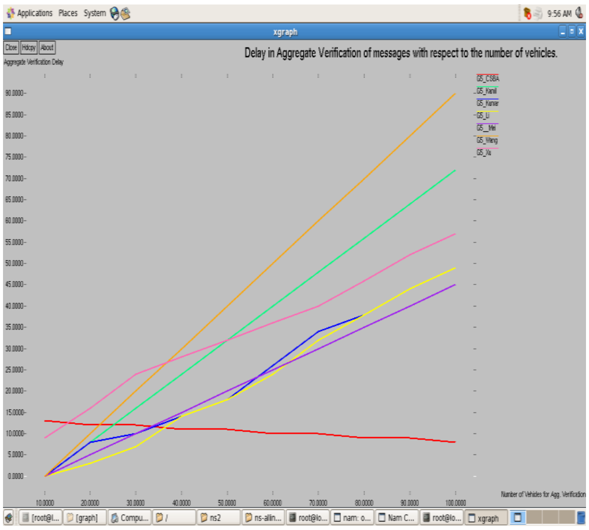

Figure 7: Delay in aggregate verification

The delay in verifying aggregated signals indicating the number of cars is seen in Figure 7.

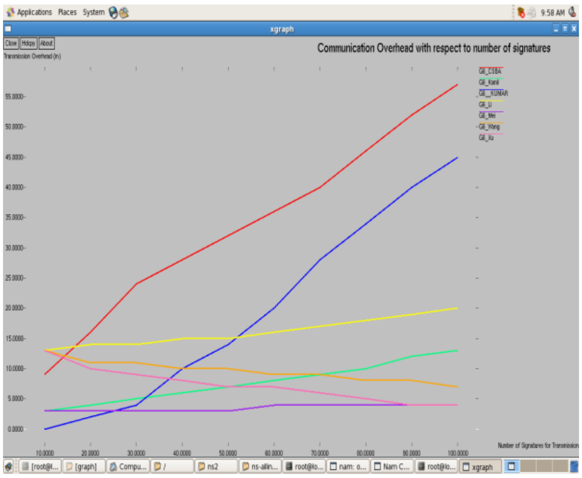

Figure 8: Communication overhead

Figure 8 illustrates the total communication overhead associated with the amount of signatures. When comparing the many authors, the CSBA approach has a significant communication cost.

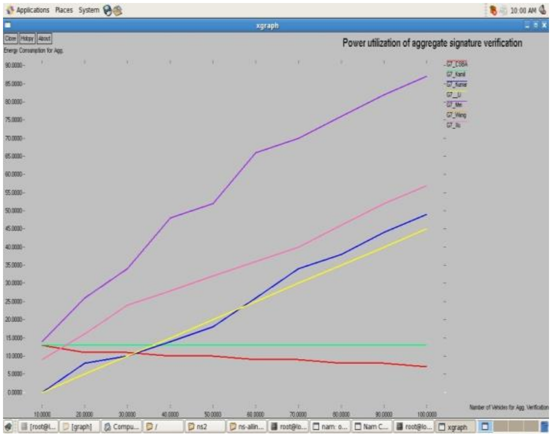

Figure 9: Power utilization

Figure 9 illustrates a comparative chart of the power consumption of aggregate signature verification. The CSBA approach consumes less energy.

5 CONCLUSIONS

This article presented a CSBA authentication mechanism that is capable of operating efficiently in the absence of permanent infrastructure along roadways. Vehicles having relative velocity and direction in the proposed protocol form groups and exchange traffic-related messages inside the network. They depend on the assistance of a group leader who can collectively validate communications and disseminate them by aggregating all messages following sufficient authentication of the message sender. While maintaining the originator's privacy and validity, CSBA significantly decreases the cost of signature verification by allowing other group members to do so. Simulations have been undertaken to validate the suggested protocol's effectiveness. Additionally, we applied blockchain technique to concentrate on trustworthy computing in VANETs.

REFERENCES

[1] Agustina, E. R., & Hakim, A. R. (2017). Secure VANET protocol using hierarchical pseudonyms with blind signature. 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). doi:10.1109/tssa.2017.8272919

[2] Celes, A. A., & Elizabeth, N. E. (2018). Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication. 2018 International Conference on Communication and Signal Processing (ICCSP). doi:10.1109/iccsp.2018.8524540

[3] Dewangan, R., Altaf, F., & Maity, S. (2019). Certificateless Aggregate Message Authentication for Hierarchical Trusted Authority based VANET. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). doi:10.1109/iccmc.2019.8819737

[4] Hu, X., Tan, W., & Ma, C. (2020). Certificateless Aggregate Signature schemes for Privacy Protection of Security Anlysis and Improvement. 2020 International Conference on Computer Science and Management Technology (ICCSMT). doi:10.1109/iccsmt51754.2020.0007

[5] Hemamalini, V., Zayaraz, G., Susmitha, V., & Saranya, V. (2017). An Efficient Probabilistic Authentication Scheme for Converging VANETs. 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM). doi:10.1109/icrtccm.2017.40

[6] Jia-Lun Tsai. (2014). An Improved Cross-Layer Privacy-Preserving Authentication in WAVE-Enabled VANETs. IEEE Communications Letters, 18(11), 1931–1934. doi:10.1109/lcomm.2014.2323291

[7] Liu, F., & Wang, Q. (2019). IBRS: An Efficient Identity-based Batch Verification Scheme for VANETs Based on Ring Signature. 2019 IEEE Vehicular Networking Conference (VNC). doi:10.1109/vnc48660.2019.9062800

[8] Lim, K., Tuladhar, K. M., Wang, X., & Liu, W. (2017). A scalable and secure key distribution scheme for group signature based authentication in VANET. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). doi:10.1109/uemcon.2017.8249091

[9] Matsukawa, T., Yamamoto, T., Fukuta, Y., Hirotomo, M., Mohri, M., & Shiraishi, Y. (2012). Controlling signature verification of network coded packet on VANET. 2012 12th International Conference on ITS Telecommunications. doi:10.1109/itst.2012.6425257

[10] Mundhe, P., Yadav, V. K., Verma, S., & Venkatesan, S. (2020). Efficient Lattice-Based Ring Signature for Message Authentication in VANETs. IEEE Systems Journal, 1–12. doi:10.1109/jsyst.2020.2980297

[11] Shao, J., Lin, X., Lu, R., & Zuo, C. (2016). A Threshold Anonymous Authentication Protocol for VANETs. IEEE Transactions on Vehicular Technology, 65(3), 1711–1720. doi:10.1109/tvt.2015.2405853

[12] Tiwari, D., Bhushan, M., Yadav, A., & Jain, S. (2016). A Novel Secure Authentication Scheme for VANETs. 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT). doi:10.1109/cict.2016.64

[13] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, Hui Li, Weidong Zhang, & Zan Li. (2013). Privacy-preserving authentication based on group signature for VANETs. 2013 IEEE Global Communications Conference (GLOBECOM). doi:10.1109/glocomw.2013.6855678

[14] Xiaodong, Y., Faying, A., Ping, Y., Likun, X., Yutong, L., Tingchun, M., & Caifen, W. (2018). A message authentication scheme for VANETs based on trapdoor hash function. 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA). doi:10.1109/icbda.2018.8367692

[15] X. Yang, R. Liu, M. Wang and G. Chen, "Identity-Based Aggregate Signature Scheme in Vehicle Ad-hoc Network," *2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, 2019, pp. 1046-10463, doi: 10.1109/ICMCCE48743.2019.00233.

[16] Yang, X., Chen, C., Ma, T., Li, Y., & Wang, C. (2018). An Improved Certificateless Aggregate Signature Scheme for Vehicular Ad-Hoc Networks. 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). doi:10.1109/iaeac.2018.8577477

[17] Zhang, C., Xue, X., Feng, L., Zeng, X., & Ma, J. (2019). Group-Signature and Group Session Key Combined Safety Message Authentication Protocol for VANETs. IEEE Access, 7, 178310–178320. doi:10.1109/access.2019.2958356