An efficient signcryption scheme for vehicular satellite-based networks

Rashad Elhabob*, Abdalla Adel[†], Nabeil Eltayieb*, Alzubier Hassan[‡], Mohamed A.H Damos[§]

*Collage of Computer Science and Information Technology, Karary University, Khartoum, 12304, Sudan
rashad@karary.edu.sd

[†] School of Information and Software Engineering, University of Electronic Science and Technology of China, China

[‡] School of Computer Science, University of Electronic Science and Technology of China, China

[§] School of GIS, Southwest Jiotong University, China

Abstract

With the widespread of the vehicular ad-hoc network (VANET), a huge number of vehicles are connecting to networks. To provide the position of these vehicles, the global position system (GPS) is required. Usually, the GPS is commoned with internal sensors mounted inside the vehicle. Thus, the communication with this sensor is needed when we need to specify the position of vehicle through the satellite. This communication is done by using a secure channels. However, the authentication and privacy are deemed as the main goal of the network communication. Therefore, an efficient signcryption scheme for vehicular satellite-based network (SVSN) is proposed in this paper. The proposed scheme meets the security demands for VANETs, for instance authentication, unforgeability, confidentiality, and integrity. Based on the Discrete Logarithm (DL) problem, the presented scheme is secure. Compared with the existing signcryption schemes, the performance analysis show that our proposed scheme is more suitable for vehicular satellite networks.

Key words-Internet of Vehicle (IoV), VANET, IoT, Signcryption, GPS

I. INTRODUCTION

With the speedy spread of technology development, the number of vehicles connected to the Internet of Things (IoT) has been increased [1], [2]. Therefore, the Internet of Vehicles (IoV) becomes a significant issue for mobile networks. These resulted in a large amount of data that needs to be collected and stored, such as vehicles speed, location, direction, etc [3], [4]. To collect these data, the vehicle should be connected and exchange the information with other components of the networks [5]. For example, to specify the position of the vehicle, the global position system (GPS) is required. The GPS is usually utilized to specify the vehicles location. Its a satellite-based navigation system, which deployed by the United State department of defense (Pentagon) [6]. At the beginning, the GPS is only used in Pentagon for the military purpose. In 1993, United States opening GPS data for civilian use [7].

At anywhere on the surface of the earth or near on it, the GPS offers approximately 7.8-meter accuracy to users [8]. To attain this goal, the 31 satellites generate signals to receivers. By using these signals, their location is determined by calculating the difference between the time of signal has been sent and received. The GPS satellites have owned atomic clocks, which provides quite an accurate time. To determine the time that the signal is broadcasted, the time information has been placed in the broadcast's codes by the satellite. Thus, the receiver can continuously get the time. Consequently, the receiver uses the data embedded in a signal to computing the locations of the satellites and then makes all of the adjustments to get the accurate positioning. To calculate the

distance between the receiver and the satellite, the receiver uses the time difference between the time of signal received and broadcasted. By the information of the three satellites ranges and the satellite's location when the signal is sent, the recipient can calculate its own three-dimensional position.

The GPS is usually combined with inertial sensors mounted inside the vehicle [9]. Thus, communication between this sensor and sink node are required. This communication is done when we need to specify the position of the vehicle, which the sensor embedded in the vehicle send message to the sink node, then the sink node communicates with the satellite-based navigation system to get the vehicle location (see Fig. 1). However, this communication is performing through the Internet. Therefore, the confidentiality, integrity, and authenticity of the data transformed are required [5], [10], [11]. An efficient privacy-preserving ride-hailing service for server providers and users has been proposed by Wang et al. [12]. By using a digital signature the authenticity and integrity of the message are achieved. In 1997, Zheng [13] presented signcryption scheme, which offers a secure communication channel. This scheme is considered useful with devices that have limited resources because the characteristics of confidentiality, authentication, integrity, and non-repudiation can be produced concurrently by the minimum cost [14]. The major feature of the signcryption is that the signature and encryption have been combined at the single logical step [15], [16], [17], which reduces the computational cost. However, all of the above-mentioned schemes are not suitable for the IoV scenario, because the limitation resource in the sensors embedded in the vehicles. Thus, in the proposed scheme, the

Fig. 1. A typical scenario for IoV.

computational cost reduced has been in the signcryption and unsigncryption phases.

A. Contribution

The contribution of this paper has been summarized as follows.

- 1) The secure communication between the sensors, sink node and satellite has been provided by proposing an efficient signcryption scheme for vehicular satellite-based networks.
- 2) To reduce the computational cost, our proposed scheme is constructed without bilinear pairing.
- 3) Eventually, compared with existing, the results show that our proposed scheme is more suitable for the IoV satellite-based scenario.

B. Organization

The rest of this paper has been organized as follows. In Section II, the related works have been presented. The definition of this paper is shown in Section III, and the construction is introduced in Section IV. The performance analysis have been presented in Section V. Eventually, the conclusion is presented in Section VI.

II. RELATED WORKS

The Internet of Vehicles paradigm is being a model for connecting vehicles, which interchanges their information through other vehicles by using vehicle-to-vehicle (V2V) and vehicle-to-roadside unit (V2R) communications [18]. However, the security and privacy of these communications should be considered [19]. Thus, an efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm has been proposed by Liu et al [20]. Liu et al. [20] proposed a broadcast authentication protocol, namely Paralleling Broadcast Authentication Protocol (PBAP), to guarantee the communication security but the proposed protocol has some drawbacks such as varying distance between vehicles and cluster-head nodes, time intervals in the alternative low-level key chain may vary as well to improve the efficiency of authentication process. However, Li et al. [21] proposed a novel authentication scheme (PPDAS) to enhance security and privacy for V2V communications in intelligent transportation systems. This system is using the broadcast authentication protocol to enhance the energy consumption, and to keep the channel communication between vehicles and wireless sensor network (WSN) secured. The public key infrastructure (PKI) currently is best paradigm tech-

nologies, which used to restrain interference in the wireless communications. Thus, PPDAS used bilinear pairing to compute encryption key. As a consequence, using bilinear pairing affect the schema performance. Therefore, the PKI is used to supply encryption, authentication, and routing operations. Furthermore, the PKI is used for digital signature regarding to provide integration and nonrepudiation [22], [23]. Hence, our paper we proposed a secure communication between the sensors, sink node and satellite using an efficient signcryption scheme which reduce the computational cost, by avoiding the use of bilinear pairing. Thus, our scheme is more suitable when it compared with the existing in term of performance.

III. DEFINITION

A. Computation assumptions

Discrete logarithm (DL) assumption:

Suppose that $\mathbb{G}$ is a group with prime order q . Assume that P is a generator of the group $\mathbb{G}$. Consider that a 2-instance (g, g^x) for a random item $x \in \mathbb{Z}_q^*$, and the DL problem is to obtain the value x . The advantage of any adversary $\mathcal{A}$ in solving the DL problem in $\mathbb{Z}_q^*$ is defined as $Adv_A^{DL} = \text{pr}[\mathcal{A}(g, g^x) = x | x \in \mathbb{Z}_q^*]$.

B. Syntax

The proposed scheme consists the following algorithms.

- 1) *Setup*: It takes as input a security parameter λ , and output a public parameters $parms$.
- 2) *Key Generation*: It takes as input public parameters $parms$, and outputs a public key pk and a secret key sk .
- 3) *Signcryption*: It takes as inputs the sender's secret key sk_s , a message m , and a receiver public key pk_r as input, and output a ciphertext C .
- 4) *Unsigncryption*: It takes as inputs a ciphertext C , sender's public key pk_s , and a receiver secret key sk_r and outputs a message m or $\perp$ if the signature is not original.

IV. CONSTRUCTION

- 1) *Setup*: Given a security parameter λ , the algorithm output public parameters $parms$ as follows.
 - Select a cyclic group $\mathbb{G}$ of a large prime order q .
 - Select g as a random generator of group $\mathbb{G}$.
 - Select $H_1 : \{0, 1\}^* \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $H_2 : \mathbb{G} \rightarrow \{0, 1\}^*$.
- 2) *Key Generation*: Upon input public parameters $parms$, the algorithm chooses $x \in \mathbb{Z}_q^*$, and outputs the key pair $(pk, sk) = (g^x, x)$.
- 3) *Signcryption*: Given the sender's secret key sk_s , a message $m \in \{0, 1\}^*$, and a receiver public key pk_r as inputs, the algorithm works as follows.
 - Select a random number $z \in \mathbb{Z}_q^*$.
 - Calculate $R = g^z$.
 - Calculate $T = pk_r^z$.
 - Calculate $E = H_1(m || R || pk_r)$.
 - Calculate $S = z^{-1}(E + xR)$.

- Calculate $C = H_2(T) \oplus (m || S)$.
- Send the ciphertext $\delta = (R, S, C)$.

- 4) *Unsigncryption*: It takes as inputs a ciphertext δ , then algorithm works as follows.

- Calculate $T' = R^{sk_r}$.
- Recover m by computing $m || S = C \oplus H_2(T')$.
- Calculate $E = H_1(m || R || pk_r)$.
- Calculate $w = s^{-1}$.
- Calculate $u_1 = E.w$, $u_2 = R.w$.
- Calculate $X = g^{u_1} pk_r^{u_2}$, and verify that if $X = R$, return m . Otherwise, reject the ciphertext.

Correctness:

$$\begin{aligned} X &= g^{u_1} pk_r^{u_2} \\ &= g^{E.w} g^{x(R.w)} \\ &= g^{w(E+xR)} \\ &= g^{z(E+xR)^{-1}(E+xR)} \\ &= g^z \end{aligned}$$

TABLE I
COMPUTATIONAL COST EVALUATION

Schemes	Signcryption	Unsigncryption	$ CT $
Mutaz et al. [24]	$4m + 1e$	$1m + 1e + 2p$	$2 \mathbb{G} + 2 \mathbb{Z}_q^* $
Zhou [25]	$3e + 1p$	$5e + 4p$	$3 \mathbb{G} + 3 \mathbb{Z}_q^* $
Our	$2e$	$3e$	$2 \mathbb{G} $

Legends: Signcryption, Signcryption computation complexity; Unsigncryption, Unsigncryption computation complexity; $|CT|$, size of the ciphertext; p , pairing operation; e , an exponentiation operation.

V. PERFORMANCE ANALYSIS

In Table I, the Signcryption computation complexity, Unsigncryption computation complexity and the size of and ciphertext of the proposed scheme (SVSN) and the schemes in [24] and [25] are compared. Our proposed schema shows the smallest Signcryption and Unsigncryption computations complexity among other schemes. Hence, our proposed schema is also the smallest size of ciphertext when compared with other schemes.

TABLE II
SYMBOLS AND RUNNING TIMES (MS).

Symbols	Characterization	Times
e	The exponentiation operation in $\mathbb{G}$	5.378
p	The pairing operation	11.370
m	The point multiplication operation	0.0282

A. Implementation

We implement our schema along with schemes that proposed in [24] and [25] based on the cpabe along with PBC library (Pairing-Based Cryptography) [26]. The specifications of the used machine is Intel(R) Core (TM) i7-7700 CPU @3.60 GHz @3.60 GHz and 8 GB RAM. Based on Windows 10 operating system and VC++ 6.0 to execute or experiment on

Fig. 2. Comparison of computation cost.

it. The implementation done using 160-bit elliptic curve group and built upon super-singular curve $z^2 = x^3 + x$ over a 512-bit finite field, to achieve a 128-bit security level. milliseconds (ms) is used to calculate the computation cost, while byte is used to calculate the cost of communication [27]. The experiment run with 11.370 ms as time for pairing operation, 0.0282 ms as point multiplication operation and 5.378 ms as time for exponentiation operation. In addition, the size of each element in bytes of G is 128, Z_p is 20. our schema is suitable in term of performance.

VI. CONCLUSION

An efficient signcryption scheme for vehicular satellite-based network (SVSN) is proposed. The proposed scheme meets the security demands for VANETs, such as authentication, integrity, unforgeability, and confidentiality. We propose SVSN scheme that is proved to be secure under the Discrete Logarithm (DL) problem. Accordingly, Our proposed scheme is Compared with the existing signcryption schemes, the performance analysis show that our proposed scheme is more suitable for vehicular satellite networks.

REFERENCES

- [1] U. Z. A. Hamid, H. Zamzuri, and D. K. Limbu, "Internet of vehicle (ioV) applications in expediting the implementation of smart highway of autonomous vehicle: A survey," in *Performability in Internet of Things*, pp. 137–157, Springer, 2019.
- [2] R. Elhabob, Y. Zhao, N. Eltayieb, A. M. Abdelgader, and H. Xiong, "Identity-based encryption with authorized equivalence test for cloud-assisted iot," *Cluster Computing*, vol. 23, no. 2, pp. 1085–1101, 2020.
- [3] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 601–610, 2017.
- [4] R. Elhabob, Y. Zhao, I. Sella, and H. Xiong, "Efficient certificateless public key cryptography with equality test for internet of vehicles," *IEEE Access*, vol. 7, pp. 68957–68969, 2019.
- [5] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.
- [6] Y. Schutz and A. Chambaz, "Could a satellite-based navigation system (gps) be used to assess the physical activity of individuals on earth?," *European journal of clinical nutrition*, vol. 51, no. 5, pp. 338–339, 1997.

- [7] C. Kaplan, "Precision targets: Gps and the militarization of us consumer identity," *American Quarterly*, vol. 58, no. 3, pp. 693–713, 2006.
- [8] N. Crato, "How gps works," in *Figuring It Out*, pp. 49–52, Springer, 2010.
- [9] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "Secure mobile health system supporting search function and decryption verification," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2221–2231, 2021.
- [10] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in iot," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 5, 2020.
- [11] A. Hassan, R. Elhabob, N. Eltayieb, and Y. Wang, "An authorized equality test on identity-based cryptosystem for mobile social networking applications," *Transactions on Emerging Telecommunications Technologies*, p. e4361, 2021.
- [12] F. Wang, H. Zhu, X. Liu, R. Lu, F. Li, H. Li, and S. Zhang, "Efficient and privacy-preserving dynamic spatial query scheme for ride-hailing services," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11084–11097, 2018.
- [13] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) / cost (signature) + cost (encryption)," in *Annual international cryptography conference*, pp. 165–179, Springer, 1997.
- [14] C. Jin, G. Chen, C. Yu, J. Shan, J. Zhao, and Y. Jin, "An efficient heterogeneous signcryption for smart grid," *PloS one*, vol. 13, no. 12, p. e0208311, 2018.
- [15] D. T. Hien, T. N. Tien, and T. T. T. Hien, "An efficient identity-based broadcast signcryption scheme," in *2010 Second International Conference on Knowledge and Systems Engineering*, pp. 209–216, IEEE, 2010.
- [16] I. T. Kim and S. O. Hwang, "An efficient identity-based broadcast signcryption scheme for wireless sensor networks," in *International Symposium on Wireless and Pervasive Computing*, pp. 1–6, IEEE, 2011.
- [17] R. Elhabob, Y. Zhao, A. Hassan, and H. Xiong, "Pke-et-hs: public key encryption with equality test for heterogeneous systems in iot," *Wireless Personal Communications*, vol. 113, no. 1, pp. 313–335, 2020.
- [18] D. B. Rawat, B. B. Bista, G. Yan, and S. Olariu, "Vehicle-to-vehicle connectivity and communication framework for vehicular ad-hoc networks," in *2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems*, pp. 44–49, IEEE, 2014.
- [19] A. Elkhailil, R. Elhabob, N. Eltayieb, et al., "An efficient signcryption of heterogeneous systems for internet of vehicles," *Journal of Systems Architecture*, vol. 113, p. 101885, 2021.
- [20] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iot paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.
- [21] M. Li, N. Ruan, H. Zhu, J. Li, and X. Li, "A paralleling broadcast authentication protocol for sparse rsus in internet of vehicles," in *2014 10th International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 58–65, IEEE, 2014.
- [22] M. Rahbari and M. A. J. Jamali, "Efficient detection of sybil attack based on cryptography in vanet," *arXiv preprint arXiv:1112.2257*, 2011.
- [23] R. Elhabob, I. Sella, Y. Zhao, G. Zhu, and H. Xiong, "A heterogeneous systems public key encryption with equality test in smart city," in *Proceedings of the 18th international conference on electronic business. ICEB, Guilin*, 2018.
- [24] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, "Hoosc: heterogeneous online/offline signcryption for the internet of things," *Wireless Networks*, vol. 24, no. 8, pp. 3141–3160, 2018.
- [25] Z. Caixue, "Certificateless signcryption scheme without random oracles," *Chinese Journal of Electronics*, vol. 27, no. 5, pp. 1002–1008, 2018.
- [26] B. Lynn et al., "The stanford pairing based crypto library," *Privacy preservation scheme for multicast communications in smart buildings of the smart grid*, vol. 324, 2013.
- [27] A. Hassan, R. Elhabob, N. Eltayieb, and Y. Wang, "An authorized equality test on identity-based cryptosystem for mobile social networking applications," *Transactions on Emerging Telecommunications Technologies*, p. e4361, 2021.