Efficient and Secure Data Aggregation for UAV-to-Ground Station Communication in Smart City Environment

Girraj Kumar Verma, Dheerendra Mishra, and Neeraj Kumar

1 Introduction

Currently, the development of smart cities is the priority of most countries. The foundation of such development is based on the utilization of Internet of things (IoT) technologies [1]. In this context, the deployment of IoT technologies helps to ensure the smart living style/standards of the citizens [2]. However, the increasing number of vehicles in smart cities has increased road accidents. According to the reports, road accidents will be the fifth leading cause of casualties by 2030 [3, 4]. Besides, the road conditions and weather conditions also increase the cost of transportation and cause the high cost of consumer items. Therefore, to ensure the smooth functioning of road traffic in smart cities, an intelligent traffic system (ITS) has been evolved [5].

In ITS, unmanned aerial vehicles (UAVs) (also called drones) are deployed to record traffic-related information. These drones can communicate with each other and also can communicate with the traffic control office (TCO). The communication between drones is called UAV-2-UAV communication and between drones to TCO is called UAV-to-Ground Station (UAV-2-GS) communication. The communication system for UAV-2-UAV and UAV-2-GS communication is utilizing the latest technologies and is called the Internet of drone (IoD) [6]. Based on the information

G. K. Verma (✉)
Amity University Madhya Pradesh, Gwalior 474005, India
e-mail: girrajv@gmail.com; gkverma@gwa.amity.edu

D. Mishra
Department of Mathematics, Maulana Ajad National Institute of Technology, Bhopal 462003, India
e-mail: dheerendra@manit.ac.in

N. Kumar
Department of Computer Science and Engineering, Thapar University, Patiala, India
e-mail: neeraj.kumar@thapar.edu

B. K. Roy et al. (eds.), *Cryptology and Network Security with Machine Learning*,
Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-99-2229-1_14

received from UAVs, TCO can update the functioning of the traffic management system. Thus, real-time feedback from UAVs causes a real-time improvement in ITS [7].

In this IoD environment, UAVs work like moving nodes in ad hoc networks. However, due to limited storage and power capacity, UAVs are resource-constrained devices. To utilize their resources in optimized manner, UAVs collect the observations from their current locations and send to TCO using a local roadside unit (RSU). This RSU is considered to have a larger space and more energy resourceful device than UAVs. Thus, some part of computation and storage is done by RSU like an edge device. In this IoD-based communication, UAVs share the information to RSU using wireless channels. Further, RSU sends the aggregated information to TCO using wired or wireless links [8].

As most of the communication links in IoD are open channels. Therefore, an unauthorized attacker can easily target the information shared. It can capture, alter, or destroy the sensitive information between UAV-2-GS communication. Sometimes, this attack on shared information can cause a serious threat. For example, attacker can modify the road condition information and send to TCO. This modified information can misguide TCO and result may be a traffic congestion [9]. As we know that traffic congestion results in a high transportation cost. Thus, the manufacture, transport company, or consumer will be in loss. Therefore, the shared information/observations should be secured from such attacks. The security in this context can be achieved by authentication and confidentiality of the data.

1.1 Signcryption and Aggregated Signcryption

To achieve authentication and confidentiality simultaneously, the paradigm of signcryption has been devised in [10]. This pioneering work by Yulian Zhang reduces the cost of encryption and then signature approach by fusing these two operations. Thus, it is suitable to deploy resource-constrained IoD-based UAV-2-GS communication. In UAV-2-GS communication, several UAVs lying in a certain region share the information to a specified TCO. Therefore, the data received from various UAVs should be processed in an efficient manner. The meaning is that the verification and decryption of received data should be performed in a single step like batch verify. To achieve the batch verification in signcryption, Selvi et al. [11] proposed the first identity-based aggregated version of signcryption. However, their scheme is utilizing costly pairing operations. Thus, it can be improved further by removing the use of pairing. In [12], Wang et al. devised a new aggregated signcryption scheme using the paradigm of multilinear maps. This scheme was the first secure in standard model. However, it has no discussion about efficiency. Further, to improve efficiency, Swapna and Reddy [13] proposed an efficient aggregated signcryption. However, still the devised construction was based on pairing. Thus further improvement can be made possible. The first pairing less identity-based aggregated signcryption has been devised in [14] by Abouelkheir and El-sherbiny. As authors have removed the use of pairing, the scheme is more efficient than previous literature. Later, some more aggregated signcryptions with more features have been devised in the literature [15–18].

1.2 Motivation and Contribution

According to the discussion, in smart city environment, utilization of ITS is the imperative need for smooth transportation. As the functioning of ITS is associated with the data received from various UAVs. Therefore, the security of communication links between UAV-2-UAV and UAV-2-GS is highly important. To secure the links, various key agreement and authentication protocols like [6–9, 19, 20] have been designed in the literature. However, in the case of UAV-2-GS link, several UAVs share information to a single TCO. Thus, to save resources at the receiving end (i.e., TCO), the verification/recovery of the received information should be done by using batch verify. The batch verify facility cannot be availed using key agreement. Therefore, key agreement schemes are insufficient to secure UAV-2-GS links. To secure these links, an efficient and secure data aggregation scheme is required. Therefore, in this paper, an efficient identity-based secure data aggregation scheme for UAV-2-GS communication has been devised. According to our sources (i.e., Internet or literature), the proposed scheme is the first scheme to secure UAV-2-GS communication in smart city ITS scenario.

The outline of the paper is as follows: next Sect. 2 presents the base definitions of foundation and related points. Section 3 introduces the proposed scheme and Sect. 4 discusses the security and efficiency analysis in brief. Section 5 concludes the paper along with future directions.

2 Preliminaries

This section introduces the basic concepts on mathematics and data aggregation in brief.

2.1 Mathematical Background

Let p and q be two primes selected randomly such that $p|(q-1)$. Suppose E be the elliptic curve defined over the finite field F_p^* and P be the generator of E. Then the following problems are defined as the base of the construction.

- *Computational Diffie–Hellman Problem (CDHP)*: Given an instance (P, aP, bP) of three elliptic points for random unknown $a, b \in F_p^*$ and it is computationally

hard to find abP. The advantage of an algorithm $\mathcal{A}$ to solve CDHP is the probability $Pr[abP \leftarrow \mathcal{A}(P, aP, bP)]$.
- *Discrete Log Problem (DLP)*: Given an instance (P, aP) of two elliptic points for random unknown $a \in F_p^*$ and it is computationally hard to find a. The advantage of an algorithm $\mathcal{A}$ to solve DLP is the probability $Pr[a \leftarrow \mathcal{A}(P, aP)]$.

The security of the proposed data aggregation relies on these computationally hard problems.

2.2 Security Attributes of the Proposed Scheme

For the proposed data aggregation between UAV-2-GS communication, the following security attributes should be considered:

- *Authentication and Integrity*: In the UAV-2-GS communication, authentication of the sender UAV (i.e., source) and data integrity is important.
- *Confidentiality*: Confidentiality of the information shared is another important attribute.
- *Man-in-the-middle (MITM) Attack*: The consideration of MITM attack is also important.

A detailed discussion regarding definition and achieving the goals will be considered in Sect. 4.2.

2.3 Threat Model

To achieve the security attributes, the semantic security along with the unforgettability of the base signcryption should be considered [21–23]. In the current settings, two types of attackers have been defined. The Type-I attacker is an honest but curious KGC. This attacker has access to master secret, however not able to replace key of a drone (user). Another attacker is Type-II, who is malicious drone (user). It has no access to master secret. The proposed scheme is said to be secure against these attackers, if no attacker wins the attack games defined in [14] corresponding to provable security. These games are played between the attacker and the challenger. In the attack games, the two types of attackers has been permitted to put requests to *Key-Gen*, *Signcryption*, and *Designcryption* oracles. The challenger can access the oracles to respond the requests. At last, the challenger can design an algorithm to solve the CDHP or DLP (for a challenged instance). For a detailed description on provable security and various attack games, please refer [14].

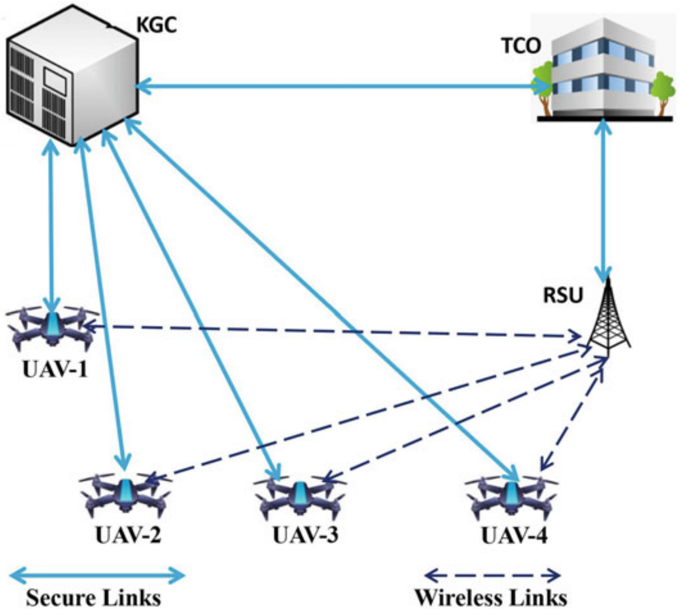

Fig. 1 System model

2.4 System Model

In the devised scheme, four entities, Key Generation Center (KGC), Traffic Control Office (TCO), UAVs, and Road Side Unit (RSU), are involved (Fig. 1). KGC generates the system parameters and keys of all the users. Generally, KGC is a UAV manufacturer company who stores the data in UAV before installation. KGC and TCO can communicate with each other using secure links. TCO is responsible for smooth functioning of ITS. For this purpose, TCO receives the data from all UAVs via RSU and use it for ITS improvement. The links between RSU-to-TCO are wired (Internet-based) links. The work of RSU is to aggregate the data received from various UAVs lying in its range. The links between UAV-2-RSU are the wireless open channels. Therefore, the communication done by using these links is the most insecure. Thus, the purpose of the proposed data aggregation is to secure this communication and to perform an efficient verification at TCO end.

3 Proposed Data Aggregation for UAV-2-GS Communication

The proposal is a modified version of the signcryption devised in [14]. The detailed steps of the scheme are follows:

- ***Initialization***: KGC runs it by input a security parameter λ and obtains the outputs as

  1. Two random primes p and q such that $p|(q-1)$.
  2. An order p subgroup $\mathcal{G}$ of elliptic curve defined by $y = x^3 + ax + b$ (where $4a^3 + 27b^2 \neq 0 \bmod p$) over $\mathbb{Z}_p^*$. P be a generator of G.
  3. Five hash functions $H_0 : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_1 : \{0,1\}^* \times G \to \mathbb{Z}_q^*$, $H_2 : G \to \mathbb{Z}_q^*$, $H_3 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times \{0,1\}^* \times G \to \mathbb{Z}_q^*$, $H_4 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times \{0,1\}^* \times G \times \mathbb{Z}_q^* \to \mathbb{Z}_q^*$.
  4. A random $s \in \mathbb{Z}_q^*$ as master secret key and $P_{\text{pub}} = sP$ as master public key.

  Final output is $params = (p, q, G, P, P_{\text{pub}}, H_0, H_1, H_2, H_3, H_4)$.
- ***Key-Gen***: Suppose, ID_i be the identity of UAV_i. KGC runs it by input $params$, ID_i and s. The steps are follows:

  1. For $x_i \in_R \mathbb{Z}_q^*$, computes $X_i = x_i P$, $S_{ID_i} = sH_0(ID_i) \bmod q$, $q_i = H_1(ID_i, X_i)$ and $d_i = (x_i + sq_i) \bmod q$.
  2. Secret key of UAV_i is (S_{ID_i}, d_i) and public key is X_i.

  KGC sends secret keys to UAV_i via secure link.
- ***Data-Aggregate***: It is done in two steps.

  - **Step 1**: For the message $m_i \in \{0,1\}^*$, the following steps are done by UAV_i:

    1. Selects $r_i \in_R \mathbb{Z}_q^*$ and computes $R_i = r_i P$ and $W_i = r_i H_0(ID_{\text{tco}}) P_{\text{pub}}$.
    2. Computes $h_{2i} = H_2(W_i)$, $h_{3i} = H_3(m_i, ID_i, X_i, W_i, ID_{\text{tco}}, X_{\text{tco}})$ and $h_{4i} = H_4(m_i, ID_i, X_i, W_i, ID_{\text{tco}}, X_{\text{tco}}, h_{3i})$.
    3. Computes $v_i = (r_i h_{3i} + d_i h_{4i}) \bmod q$ and $V_i = v_i P$.
    4. Computes $C_i = (m_i \| v_i) \oplus h_{2i}$.

    After this, UAV_i sends $\sigma_i = (C_i, R_i, V_i)$ to RSU.
  - **Step 2**: RSU receives data from n UAVs and computes $V = \sum_{i=1}^{n} V_i$.
  - RSU forwards $\sigma_{\text{agg}} = ((C_1, C_2, \ldots, C_n), (R_1, R_2, \ldots, R_n), V)$ to TCO as aggregated data.

- ***Verify-Decryption***: The following steps are done by TCO:

  1. For $1 \leq i \leq n$, compute $W_i = S_{ID_{\text{tco}}} R_i$ and recover $m_i \| v_i = C_i \oplus H_1(W_i)$.
  2. Checks $V = \sum_{i=1}^{n} h_{3i} R_i + \sum_{i=1}^{n} h_{4i} X_i + (\sum_{i=1}^{n} h_{4i} q_i) P_{\text{pub}}$.

  If equation holds, accept the ciphertexts as valid.

4 Security and Efficiency Discussion

4.1 Correctness

From the construction of the scheme, $V = \sum_{i=1}^{n} V_i$, where $V_i = (r_i h_{3i} + d_i h_{4i})P$, $h_{3i} = H_3(m_i, ID_i, X_i, W_i, ID_{\text{tco}}, X_{\text{tco}})$ and $h_{4i} = H_4(m_i, ID_i, X_i, W_i, ID_{\text{tco}}, X_{\text{tco}}, h_{3i})$. Therefore, $V = \sum_{i=1}^{n}(r_i h_{3i} + d_i h_{4i})P$, i.e., $V = \sum_{i=1}^{n} h_{3i} R_i + \sum_{i=1}^{n} h_{4i} X_i + (\sum_{i=1}^{n} h_{4i} q_i) P_{\text{pub}}$ as $d_i = (x_i + sq_i) \bmod q$. Thus, the Verify-Decryption runs correctly.

4.2 Security Attributes Analysis

As per the discussion in Sect. 2.2, the proposed scheme satisfies the following attributes:

- *Authentication and Integrity*: In the designing of the protocols, during *Data-Aggregate* phase, each UAV$_i$ computes ciphertext $C_i = (m_i \| v_i) \oplus h_{2i}$, where $v_i = (r_i h_{3i} + d_i h_{4i}) \bmod q$. This computation is possible with secret key d_i of the UAV_i. At the receiver end, i.e., TCO, verification needs to check $V = \sum_{i=1}^{n} h_{3i} R_i + \sum_{i=1}^{n} h_{4i} X_i + (\sum_{i=1}^{n} h_{4i} q_i) P_{\text{pub}}$. This step is possible only with public key X_i of UAV$_i$ and secret key $S_{ID_{\text{tco}}}$ of TCO. Thus, the generation of ciphertext can be done by legitimate UAV_i only. From the discussion in [14], the base scheme is unforgettable, and therefore authentication is satisfied. For verify purpose, secret key of TCO is needed, so alteration of message is not possible, i.e., integrity is also satisfied.
- *Confidentiality*: As per the scheme [14], the encryption is semantically secure. Therefore, an adversary is unsuccessful to get any observation from the ciphertext. Thus, confidentiality is also satisfied.
- *MITM Attack*: As the base scheme [14] is unforgettable against an adaptively chosen message attack. Besides, the possible alteration to ciphertext will result in rejection during verification/decryption process. Thus, no adversary can impersonate the signer or cannot modify the content. Thus, the scheme is secure against MITM attack.

4.3 Efficiency Analysis

The computational costs of various cryptographic operations have been referred from [24] (shown in Table 1). In the literature, a limited resource device single 798 MHz CPU has been utilized with 256 MB RAM support. Thus, it can be a good choice to emulate an UAV capacity. Based on the discussion, UAVs are resource-

Table 1 Computation costs of various cryptography operations [24]

Operation	OBU/RSU (ms)
Bilinear pairing	67.32
Modular exponentiation	7.87
Modular multiplication	21.63
Hash	0.025
Pairing multiplication	21.63
Scalar multiplication	14.83
Map to point hash	5.23
Elliptic point addition	4.61

constrained devices. UAVs are having less storage capacity, less computation capacity, and limited power backup. Thus, the computation done by UAVs is analyzed. During the ciphertext generation phase, 3 scalar multiplications + 3 modular multiplications + 3 hash functions are computed. The total cost of these operations is $3 \times 14.83 + 3 \times 21.63 + 3 \times 0.025 = 109.455$ ms. Thus, it is not a very big computation time for a resource-constrained device like UAV. If the computation overhead of RSU is considered, it is $\approx (n-1)4.61$ ms. As RSU is stronger than UAV, it is adjustable computation. Similarly, the cost incurred by TCO is $\approx (66.195n - 6.8)$ ms. It is also not a large consumption time for TCO as it has infinite resources. Therefore, the proposed scheme is practically suitable for UAV-2-GS communication with respect to computational efficiency.

5 Conclusion

Based on the various reports, it is observed that road accidents and traffic congestion are big losses to the world economy. In smart city environment, UAVs are utilized to get real-time traffic data. This data enhances the functioning of ITS by inserting the feedback analysis. However, the links between UAV-to-TCO are wireless. Thus, a secure data aggregation based on a signcryption scheme has been proposed in this paper. The security and efficiency analysis presents the suitability of the proposal for UAV-2-GS communication.

As a future scope, data aggregation for multiple applications using UAV-2-GS communication should be devised.

References

1. Misra MK, Chaturvedi A, Tripathi SP, Shukla V (2019) A unique key sharing protocol among three users using non-commutative group for electronic health record system. J Discret Math Sci Cryptogr 22(8):1435–1451
2. Shukla V, Chaturvedi A, Misra MK (2021) On authentication schemes using polynomials over non commutative rings. Wirel Person Commun 118(1):1–9
3. WHO, Global status report on road safety. https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries#:~:text=Every%20year%20the%20lives%20of,a%20result%20of%20their%20injury. Accessed 08 May 2022
4. European Commission (2021) Road safety thematic report—Fatigue. European Road Safety Observatory. Brussels, European Commission, Directorate General for Transport. https://ec.europa.eu/transport/road_safety/system/files/2021-07/asr2020.pdf. Accessed 08 May 2022
5. Raya M, Hubaux J-P (2005) The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks, pp 11–21
6. Gope P, Sikdar B (2020) An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. IEEE Trans Veh Technol 69(11):13621–30
7. Alladi T, Chamola V, Kumar N (2020) PARTH: a two-stage lightweight mutual authentication protocol for UAV surveillance networks. Comput Commun 160:81–90
8. Alladi T, Bansal G, Chamola V, Guizani M (2020) SecAuthUAV: a novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Trans Veh Technol 69(12):15068–77
9. Srinivas J, Das AK, Kumar N, Rodrigues JJ (2019) TCALAS: temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. IEEE Trans Veh Technol 68(7):6903–16
10. Zheng Y, Digital signcryption or how to achieve cost (signature & encryption) $<<$ cost (signature)+ cost (encryption). In: Annual international cryptology conference. Springer, Berlin, Heidelberg, pp 165–179
11. Selvi SSD, Vivek SS, Shriram J et al (2009) Identity based aggregate signcryption schemes. In: Progress in Cryptology—INDOCRYPT, Lecture Notes in Computer Science, Poland, pp 378–397
12. Wang H, Liu Z, Liu Z, Wong DS (2016) Identity-based aggregate signcryption in the standard model from multilinear maps. Front Comput Sci 10(4):741–54
13. Swapna G, Reddy PV. Efficient identity based aggregate signcryption scheme using bilinear pairings over elliptic curves. J Phys: Conf Ser 1344(1):012010 (IOP Publishing)
14. Abouelkheir E, El-sherbiny S (2020) Pairing free identity based aggregate signcryption scheme. IET Inf Secur 14(6):625–632
15. Shukla V, Srivastava N, Chaturvedi A (2016) A bit commitment signcryption protocol for wireless transport layer security (wtls). In: IEEE international conference on electrical, computer and electronics engineering, pp 83–86
16. Yang X, Zhou H, Ren N, Tian T. Homomorphic proxy re-signcryption scheme and its application in edge computing-enhanced IoT. In: 2021 2nd international conference on electronics, communications and information technology (CECIT). IEEE, pp. 644–649
17. Yu H, Ren R (2021) Certificateless elliptic curve aggregate signcryption scheme. IEEE Syst J 16(2):2347–54
18. Yang Y, He D, Vijayakumar P, Gupta BB, Xie Q (2022) An efficient identity-based aggregate signcryption scheme with blockchain for IoT-enabled maritime transportation system. IEEE Trans Green Commun Netw
19. Zhang Y, He D, Li L, Chen B (2020) A lightweight authentication and key agreement scheme for internet of drones. Comput Commun 15(154):455–64
20. Wazid M, Das AK, Kumar N, Vasilakos AV, Rodrigues JJ (2018) Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. IEEE Internet Things J 6(2):3572–84

21. Chaturvedi A, Shukla V, Misra MK (2021) A random encoding method for secure data communication: an extension of sequential coding. J Discrete Math Sci Cryptogr 24(5):1189–1204
22. Shukla V, Chaturvedi A, Srivastava N (2019) A new one time password mechanism for client-server applications. J Discrete Math Sci Cryptogr 22:1393–1406
23. Shukla V, Misra MK, Chaturvedi A (2021) A new authentication procedure for client-server applications using HMAC. J Discrete Math Sci Cryptogr 24(5):1241–1256
24. Verma GK, Gope P, Kumar N (2022) PF-DA: pairing free and secure data aggregation for energy internet-based smart meter-to-grid communication. In: IEEE Trans Smart Grid 13(3):2294–2304