2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&amp;PW) | 979-8-3503-6729-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/EUROSPW61312.2024.00049

Secure, Robust, and Energy-Efficient Authenticated Data Sharing in Drone to Vehicles Communications

Atefeh Mohseni Ejiyeh
University of California, Santa Barbara, USA
atefeh@ucsb.edu

Abstract—**In response to the need for reliable and secure communication systems to ensure public safety in sixth-generation (6G) wireless networks, this paper addresses the challenges of utilizing drones (Unmanned Aerial Vehicles or UAV) for vehicle-to-vehicle (V2V) communication. While 6G networks promise rapid data delivery with minimal latency, ensuring consistent connectivity poses a significant challenge, particularly in scenarios vital for public safety. To mitigate these challenges, we propose integrating drones into the communication infrastructure. Our novel approach involves drones collaboratively retrieving content from service providers and establishing secure connections with vehicles to facilitate secuer and efficient data exchange. We propose two innovative protocols: SeGDS for coordinated group data retrieval among drones, and SeDDS for secure direct data sharing with vehicles. These protocols offer lightweight, certificate-free solutions with features such as vehicle revocation, non-repudiation, and mutual authentication. Emphasizing high availability, our protocols effectively detect and mitigate Denial of Service (DoS) and free riding attacks. This ensures robust security for UAV swarm deployments and public safety. Furthermore, we evaluate the energy efficiency of our proposed protocols, demonstrating their effectiveness in reducing energy consumption compared to existing methods. Specifically, SeDDS reduces computation overhead by 1.5x, while SeGDS decreases communication costs by 2.5x. Leveraging certificateless signcryption and certificateless multi-receiver encryption, our protocols for the first time provide a comprehensive solution for securing and enhancing communication in 6G networks, critical for public safety and mission-critical services.**

Index Terms—**Unmanned Aerial Vehicle (UAV), VANET, V2X, Group data downloading, Zero-Trust, Certificateless, Signcryption, 6G**

1. Introduction

The sixth generation of wireless communication networks (6G) brings a significant advancements in connectivity. These advancements include lightning-fast data delivery speeds of up to 1 Tbps, marking a notable hundred-fold increase over the capabilities of its predecessor, 5G. Moreover, 6G exhibits ultra-low latency, with response times reaching below 100 milliseconds, and demonstrates significantly enhanced energy efficiency [1]. These remarkable features hold the potential to revolutionize various aspects of communication technology, enabling transformative applications ranging from real-time immersive experiences to the establishment of resilient emergency networks. However, realizing these ambitious objectives necessitates the development of innovative infrastructure solutions.

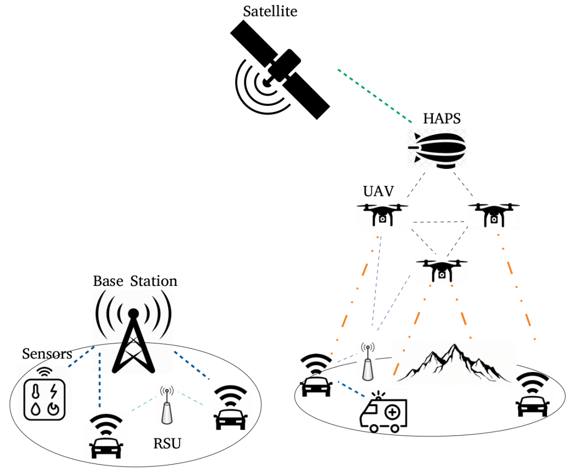


Figure 1. The architecture of UAV-assisted networks in B5G/6G (HAPS: High Altitude Platform System, UAV: Unmanned Aerial Vehicles, RSU: Road Side Unit)

Traditionally, network coverage in terrestrial environments has been predominantly handled by terrestrial base stations. However, these base stations often face limitations, particularly in scenarios that demand ubiquitous connectivity, such as disaster response efforts or communication in remote areas. In response to these challenges, unmanned aerial vehicles (UAVs), commonly known as drones, have emerged as a viable solution [2]. Leveraging their dynamic mobility and adaptability, as illustrated in Figure 1, UAVs are capable of filling coverage gaps and dynamically adjusting network resources to meet critical service delivery needs.

UAVs demonstrate immense potential in providing emergency networking capabilities in the aftermath of natural disasters [3]. Their ability to rapidly deploy and establish temporary communication infrastructure in disaster-stricken areas can significantly improve response times and facilitate coordination efforts among emergency responders. Overall, UAVs represent a versatile and adaptable solution for extending network coverage and enhancing communication resilience in various challenging environments.

In the context of UAV-assisted Vehicular Ad-hoc Networks (VANETs), the integration of UAVs introduces new dimensions to the network architecture and opera-

DOI 10.1109/EuroSPW61312.2024.00049

tion. VANETs are characterized by highly dynamic and mobile nodes, such as vehicles, which require seamless and reliable communication for various applications, including traffic management, collision avoidance, and infotainment services. However, traditional terrestrial infrastructure may face limitations in providing comprehensive coverage, especially in areas with sparse or no network coverage. UAVs offer a promising solution to address these coverage challenges by providing on-demand aerial connectivity and augmenting the existing terrestrial infrastructure [4]. Their ability to rapidly deploy and adapt to changing network conditions makes them well-suited for enhancing communication resilience and extending network coverage in VANETs [5]. By leveraging UAVs in VANET environments, it becomes possible to achieve more robust and efficient data sharing protocols, facilitating improved traffic management, enhanced safety measures [6], and seamless connectivity for vehicles on the move.

However security concerns of UAV-assisted networks remain in their infancy [7]. Notably, recent studies identified vulnerabilities to localization attacks [8], and lack of robust access control and authenticated message exchange among UAVs [9]- [10]. However, realizing the full potential of these networks hinges on addressing a central challenge: establishing secure communication channels among entities [11]. This is particularly crucial as UAVs collaborate to download data for performance enhancement and service delivery. Unsecured channels pose a significant risk, exposing sensitive data to interception and manipulation, thereby compromising data privacy and network integrity. Moreover, ensuring reliable data delivery to end-users is paramount for minimizing delays and errors, especially in real-time applications and emergency networks.

This paper addresses both challenges by presenting two innovative protocols for secure and energy-efficient content sharing in UAV-assisted VANETs.

- **Group Data Sharing Protocol** enables efficient content sharing among collaborating UAVs by downloading data packets, minimizing redundancy, and expediting delivery.
- **Direct Data Sharing Protocol** ensures secure and non-repudiable direct data sharing between UAVs and vehicles, eliminating intermediate hops for tamper-proof transmission without third-party intervention.

By meticulously analyzing the security, performance, and overhead of these protocols against state-of-the-art, we showcase their superiority. This research establishes the groundwork for resilient and dependable communication channels in the evolving 6G era, unlocking the potential of UAV-assisted VANETS.

2. Background

2.1. Extensible Authentication Protocol (EAP) in Beyond 5G

In the context of 5G and emerging 6G networks, Extensible Authentication Protocol with AKA (EAP-AKA) is pivotal for secure User Equipment (UE) authentication. This process centers around the Authentication Server Function (AUSF), a central entity managing user identities and cryptographic keys. EAP-AKA involves a cryptographic handshake initiated by the UE (or UAV), with the AUSF verifying the identity using a shared secret, establishing trust for encrypted communication. The AUSF's dual role includes issuing unique device IDs for verification in distributed protocols and facilitating high-level authentication for access to sensitive data [12]. In our proposed protocols, UAVs and vehicles use legitimate network IDs for registration in the data sharing schemes detailed in Sec 3.

2.2. Cellular-assisted V2V Communications

Cellular networks enables direct interaction between nearby devices called Device-to-device (D2D) communication, providing benefits like improved latency and personalized content delivery. In cellular-controlled D2D, the base station manages connections for optimal network performance. Unlicensed-spectrum-based channels, utilizing Wi-Fi Direct or Bluetooth, offers autonomy and flexibility [13]. D2D applications extend beyond mobile networks; Swarm UAVs group nearby UAVs for efficient content sharing [14]- [2], and Cellular-Assisted V2X enhances direct communication between vehicles for improved safety and traffic management [15]. In this paper, we introduce a novel secure authentication and message exchange protocol for unlicensed-spectrum D2D, a first in the field. Additionally, we present a cluster-based D2D protocol operating on licensed spectrum, enhancing secure collaborative content sharing among UAVs in proximity.

2.3. Certificateless Signcryption

Certificateless signcryption (CL-signcryption) offers a cryptographic primitive combining digital signature and encryption functionalities into a single operation. Instead of relying on pre-issued certificates, users derive their keys based on their identities, simplifying key management compared to certificate-based schemes. CL-signcryption offers three main functionalities:

1) **Signature**: It allows a user to prove ownership of their identity while authenticating data integrity and non-repudiation.
2) **Encryption**: It enables secure data confidentiality by encrypting information for specific intended recipients using their identities.
3) **Signcryption**: It combines both functionalities, simultaneously signing and encrypting data for authenticity and confidentiality in a single step.

In this paper, we employed [16] for its efficient certificateless signcryption functionalities.

2.4. Certificateless Multireceiver Encryption

Certificateless Multireceiver Encryption is a cryptographic approach devised to secure data transmission in multicast scenarios without the need for traditional public key certificates. It addresses scalability and efficiency challenges inherent in conventional multicast encryption by streamlining the key distribution process.

1) **Multireceiver Encryption (CL-MREnc)**: Sender utilizes the group leader's public key and unique identifiers for each recipient, then generates a multicast session key for encrypting the data, ensuring confidentiality.
2) **Multireceiver Decryption (CL-MRDec)**: Recipient employs their unique identifier and private key to derive the multicast session key.

CL-MREnc streamlines key management, improves scalability, and offers an effective solution for secure multicast communication, notably advantageous in scenarios like UAV-assisted networks. Here, we leverage [17] for the proposed secure collaborative data sharing scheme detailed in Sec. 3.

2.5. Threat Model

Adhering to the Dolev-Yao threat model [18], adversaries possess the capability to intercept messages transmitted through public channels, initiate and receive conversations with other participants, and engage in entity impersonation. We assume the Service Provider (Cloud) operates honestly and provides the original content. Similarly, the Road Side Unit (RSU) is trusted with monitoring the behavior of UAVs and revoking credentials from consistently misbehaving UAVs. UAVs are considered rational entities with limited resources, behaving maliciously only when there's a perceived benefit. Collisions among adversaries are possible.

3. SeGDS: Secure Group Data Sharing Scheme

In this section, the proposed cooperative data sharing protocol is explained step by step. It is assumed that the group members have been informed about the identity and public key of the RSU acting as a leader for a collaborative data downloading session.

TABLE 1. NOTATION DEFINITIONS

Term	**Description**
CSP	Content Service Provider
FN, FS	File Name, File Segment
$CLGSC(ID_i, 0, *)$	Signature of entity with ID_i
$CLGSC(ID_i, ID_j, *)$	Signcryption of entity with ID_i to ID_j

3.1. System Initialization Phase

AUSF selects a cycle group G with generator P on an elliptic curve with two prime numbers p, and q given the security parameter k. Additionally, the AUSF selects x_0 as the private master key and $Q = x_0 P$ as the public master key. The four hash functions are selected as $H_0 : \{0,1\}^* \times G \times G \times G \rightarrow Z_q^*$, $H_1 : G \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$, $H_2 : G \times G \rightarrow \{0,1\}^n$, and H_3 equivalent to SHA-256. The utilized symmetric encryption function is AES-256.

3.2. Registration Phase

UAVs submit membership requests containing their identifier (ID_i), partial secret key $x_i \in Z_q^*$ for $i >= 1$, and public partial key $X_i = x_i P$. The AUSF operation verifies these requests, ensuring access authorization and UAV authentication. Following successful verification, the AUSF encrypts the UAV's partial keys (z_i, Y_i) as $z_i = y_i + x_0 H_0(ID_i, Y_i, X_i, X_0)$ when $y_i \in Z_q^*, Y_i = y_i P$ and transmits them through a secure channel. The full private key of the entity with ID_i is (x_i, z_i). A similar registration process is followed for vehicles.

3.3. Session Setup Phase

The designated RSU establishes a secure session with the content service provider. It involves sharing the target file name FN and generating a data encryption key (K_d) through Diffie–Hellman key exchange protocol. Consequently, the content server provider utilizes K_d to encrypt each segment of the file which will be requested by UAVs in the downloading phase.

3.4. Task Assignment and Cooperative Download Phase

RSU distributes downloading tasks among group members equally or in varied sized segments given the total file size and UAVs QoS.

Step 1: RSU divides the target file segments among members. Messages sent to UAVs, e.g., UAV with ID_i is $M_1 : (ID_{RSU}, ID_i, FN, FS, T_s, CLGSC(RSU, 0, *))$ indicate a file segment FS to be downloaded by UAV_i. The timestamp T_s marks task assignment, and the RSU's signature on the message is represented by $CLGSC(RSU, 0, *)$.

Step 2: UAV_i verifies the RSU's signature upon receiving the message. Upon confirmation, the UAV forwards the message to the content service provider to download their assigned portion of the file.

Step 3: The content service provider, upon receiving the UAV's request, verifies the freshness of the timestamp and the validity of the RSU's signature on the message. Upon confirmation, it encrypts the relevant segment of the file data associated with FS with K_d and delivers it to the UAV_i as $M_2 : (ID_{SP}, ID_i, FN, FS, C_i, T_s, \sigma_{sp} = CLGSC(SP, 0, H_3(C_i || *)))$ where $C_i = Enc(K_d, M_i)$.

3.5. Data Sharing Phase

In this phase, each UAV shares their downloaded segment with other UAVs in the group as well as verifying and accepting received messages. After completing the download of FS, each UAV verifies the content service provider's signature. If confirmed, it appends the download completion timestamp (T_d) and broadcast it among all members as $M_3 = (M_2, T_d, \sigma_i = CLGSC(ID_i, 0, (M_2 || T_d))$. Each member verifies received messages and accepts the segment data upon confirmation. The RSU is responsible for verifying messages exchanged within the group, and maintains a blacklist for UAVs shared invalid messages. If a UAV fails to perform their assigned task within a specified time window, the RSU can assume non-cooperation and adds their ID to the blacklist depends on the record of the UAV in the system. If any data segments remains, the RSU repeats 3.4 steps.

3.6. Data Consolidation Phase

After downloading all the file segments, the RSU encrypts the file encryption key K_d using a multi-receiver encryption scheme and distributes it among members as $M_4 : (CL - MREnc(K_d), T_f, GLGSC(RSU, 0, *))$. Any UAV added to the RSU's blacklist should not be able to decrypt the key value. Upon receiving the message, each member verifies the signature, checks the freshness of the timestamp T_f, and decrypts the data using CL-MRDec with the acquired data key through $M_i = Dec(K_d, C_i)$. Finally, UAV decrypts the file content after obtaining the symmetric encryption key K_d.

Following the completion of the SeGDS protocol, the UAVs are equipped with the data and have the flexibility to relocate to areas where the RSU anticipates a demand for this information, whether for data offloading to alleviate traffic load from the base station or for emergency response scenarios.

4. SeDDS: Secure Direct Data Sharing scheme

In the following section, the SeDDS protocol is presented, which enables direct data sharing between UAVs and vehicles. We presume vehicles to be registered, as outlined in 3.2, before they can receive services within the system. Here's the data sharing steps after a vehicle discovered the presence of a UAV nearby.

Step 1: VID_i sends a data download request to UAV_j through $(VID_i||ID_j||FN||T_s||g^a||GLGSC(VID_i, 0, *))$ which FN describes desired file name, and g^a generated following the Diffie-Hellman key exchange protocol with $a \in Z_q^*$.

Step 2: UAV_j verifies the validity of the received request; then chooses a random $b \in Z_q^*$, and computes $k_c = (g^a)^b$. UAV_j encrypts the content M associated with FN through $C' = Enc(k_c, M)$, and transmits the cipher data as $(ID_j||VID_i||C'||T_s||\sigma_{sp}||\sigma_j = GLGSC(ID_j, 0, *)))$ to VID_i in which σ_{sp} shows the original signature of the service provider on the file.

Step 3: By receiving the message of UAV_j, VID_i verifies the σ_j: if it holds true, VID_i sends a "key hint" request to the UAV_j containing $(VID_i||ID_j||FN||T_s||T_i||FN \oplus h(C')||\sigma_{i,1} = CLGSC(VID_i, 0, *)$. The inclusion of $FN \oplus h(C')$ in this request serves the purpose of adhering to the non-repudiation feature of the protocol, preventing VID_i from denying the service received later on.

Step 4: Upon receiving a key hint request, UAV_j sends the data encryption key to VID_i. To mitigate payment risk and enhance user experience, a prepayment strategy is employed. VID_i is subject to pay a portion of the credits ($0 < p < 100$) after receiving the encrypted data in step 3. Only if VID_i verifies the data's originality, UAV_j informs the service provider about the full credit charges. UAV_j sends a message like $(ID_j||VID_i||g^b||FN||\sigma_j = CLGSC(ID_j, 0, *))$ to VID_i.

Step 5: VID_i calculates the data encryption key using $(g^b)^a$ and decrypts C'. It verifies the signature of the service provider, σ_{sp}. If the signature is valid, VID_i sends a message $(VID_i||ID_j||FN||FN \oplus h(M)||T_i||\sigma_{i,2} = CLGSC(VID_i, 0, *))$ back to the UAV_j.

This concludes a secure data exchange between a UAV and vehicle. Note that SeDDS can perform offline in areas that UAVs or vehicles dont receieve network coverage. Whenever UAV_j is online can forward the Ack message from VID_i to the service provider. AUSF checks the validity of VID_i's signatures. If verified, it computes a hash of the original content FN through $(M \oplus h(C'))$. If UAV_j has only received $\sigma_{i,1}$ and the XOR result doesn't match, it indicates a failed connection. Conversely, if VID_i has received $\sigma_{i,2}$, it signifies a successful data transfer. Moreover, the protocol can be extended to facilitate data exchange between two vehicles, thereby alleviating the load on UAVs. AUSF might maintain anonymized records of vehicle content possessions for incentivization purposes, proximity-based services, and to reward vehicles for active participation.

5. Performance Analysis

In the subsequent sections, we quantify the computation and communication overhead introduced by our protocols and compare them with state-of-the-art. The evaluation metrics utilized in this study are based on those outlined in [19] which is measured for 5G-enabled VANETS similar to our system model. The cryptographic functions listed in Table 2 were assessed using the MIRACL [20] and PBC [21] libraries, implemented in C/C++, and executed on an Intel i7-7500U CPU operating at a frequency of 2.70 GHz, with 8 GB of RAM. For simplicity, negligible operations, such as hash functions, have been omitted. Given that UAV-assisted secure data sharing remains an active area of research [9], we compare our proposed protocols with related schemes in VANET, as illustrated in Figures 2 and 3.

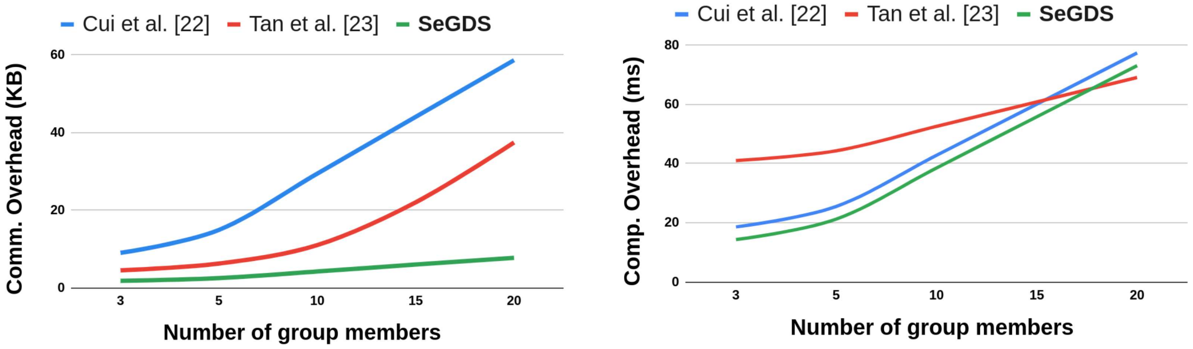
TABLE 2. COMPUTATION COST OF UNDERLYING CRYPTOGRAPHIC OPERATIONS

Operation	Detail	Time (ms)
T_e	Modular exponential operation (1024 bits)	0.249
T_m	Scale multiplication related to elliptic curve	0.576
T_{bp}	Bilinear pairing	6.574
T_{sm}	Scale multiplication related to a bilinear group	2.132
T_{AES_E}	AES-256 encryption	0.53
T_{AES_D}	AES-256 decryption	7.425
T_{RSA_G}	RSA signature generation	12.56
T_{RSA_V}	RSA signature verification	0.45
T_{RSA_E}	RSA encryption	0.43
T_{RSA_D}	RSA decryption	12.45

5.1. SeGDS Scheme Performance

5.1.1. Computation Overhead.

- **UAV** In the task assignment phase, the UAV verifies the RSU's signature using the CLGSC scheme [16], taking T_m for verification. Subsequently,



(a) Group Communication Overhead Comparison in Kilobyte

(b) Group Computation Overhead Comparison in millisecond

Figure 2. Performance Evaluation of SeGDS Scheme vs. State of the Art

TABLE 3. COMPARATIVE COMPUTATION AND COMMUNICATION OVERHEAD IN GROUP DATA SHARING SCHEMES (N MEMBERS=5)

Scheme	Computation Cost (ms)	Comm. Cost (bytes)
Cui et al. [22]	$13T_m + 3T_e + 6NT_m$ = 25.51	2912N+362 = 14.9K
Tan et al. [23]	$32T_m + 2T_{bp} + 18T_e + 2N(T_m + T_e)$ = 44.31	1250N = 6.25K
SeGDS	$6(N+1)T_m + 2T_e$ = **21.23**	360N+782 = **2.5K**

UAVs sign and share their assigned file segments, each taking T_m, and verify messages received from the group, collectively taking $(N-1)T_m$. Upon data consolidation, each UAV verifies the RSU's signature on message M_4 within T_m, and decrypts it using CL-MRDec [17] within T_m to obtain the data encryption key K_d. UAV then decrypts the file content within T_{AES-D}.

- **RSU** The RSU spends T_e to generate a half key of the Diffie-Hellman scheme for sharing with the CSP during the session setup phase, and signs its request within T_m. During task assignment, the RSU signs task messages to group members, requiring $N \times T_m$. Finally, the RSU encrypts the data encryption key K_d using CL-MREnc [17], taking $(2N+1)T_m$.
- **CSP** The CSP verifies the RSU's group download session request within T_m, generates the data encryption key (using Diffie-Hellman) within T_e, encrypts the file content within T_{AES-E}, and subsequently verifies each UAV's download request signature within T_m. The encrypted data is then sent, requiring CSP's signature in $N \times T_m$.

5.1.2. Communication Overhead. We utilized AES-256 for encryption and CLGSC [16] for signatures, entity IDs, file names (FN), file segments (FS), and Timestamps, each considered to be 2 bytes.

- **UAV** UAVs forward the download request to the CSP, which is 70 bytes in length. They also share the received downloaded segment, signed, with other members, totaling C_i + 200 bytes.
- **RSU** The RSU initiates a group session with the CSP, requiring 92 bytes. It then sends a task delegation request to members, each taking 70 bytes. During the data consolidation phase, the RSU shares the data encryption key (from CL-MREnc scheme) with members, requiring $(N+2)\times20+32+60+2$ bytes. Therefore, the total communication overhead for the RSU is $226+90N$ bytes.
- **CSP** The CSP shares the file segments message to UAVs, which takes 70 + C_i bytes (C_i represents the length of the encrypted file segment using AES). Additionally, the CSP signs the message. Thus, the total overhead for the CSP is $70N+C$, where C is the total encrypted size of the file FN.

5.1.3. Overhead Comparison. The summary of SeGDS overhead is presented in Table 3 with comparison to similar schemes [22] and [23] which described below.

Cui et al. [22] introduced a secure cooperative data downloading scheme leveraging edge computing in VANETS. The method relies on RSUs caching popular data in nearby edge computing vehicles (ECVs), facilitating direct downloads by vehicles. However, the assumption of sufficient available qualified ECVs without resource constraints and the high communication overhead making it impractical for dynamic and UAV-assisted emergency networks.

Tan et al. [23] present a certificateless mutual authentication protocol for UAV group association, employing a shared partial secret key for secure UAV group key generation, updates, and dynamic revocation. They suggest a method for remote V2V message dissemination through decentralized edge RSUs, relying on pre-stored records. However, the scheme's dependence on vehicular cloud authentication and the assumption of an existing wired RSU cluster constrain its practicality, particularly for emergency networks.

Hence, the proposed Secure Group Data Sharing scheme reduces the total communication expenses by 2.5 times, as shown in Table 3. Note: T_{AES} encryption and decryption times are excluded from all schemes listed in table for simplicity.

5.2. SeDDS Scheme Performance

5.2.1. Computation Overhead.

- **UAV** The UAV expends T_e to compute its half of the Diffie-Hellman key exchange in step 2. It also allocates $4 \times T_m$ for verifying vehicle messages, signing its own message, and T_{AES-E} for encrypting the file using the data session key.
- **Vehicle** VID_i generates the half Diffie-Hellman key within T_e. In total, it spends $6 \times T_m$ to sign or verify signatures of UAV_j and CSP. VID_i also requires T_{AES-D} to decrypt the file at the end.

5.2.2. Communication Overhead. Similarly, identities, timestamps, and file identifiers each take two bytes. The signature scheme utilized [16] accounts for 60 bytes, while the hash function is SHA-256 (32 bytes).

- **UAV** The message in step 2 contains C', assumed to take L bytes, and the rest of the messages sent by the UAV amount to $L + 216$ bytes.
- **Vehicle** The message sent in step 1 by VID totals 88 bytes. Messages sent in steps 3 and 5 include the SHA-256 hash of the message, adding 32 bytes. The total overhead for a vehicle is 292 bytes.

5.2.3. Overhead Comparison. Table 4 summarizes the overhead of the SeDDS scheme in comparison with similar works. Please note that the size of the encrypted file L has not been listed for all schemes for simplicity.

To the best of our knowledge, there is no secure direct data sharing scheme that assumes no trust between entities and can be run offline. The following are similar works to SeDDS:

HDMA [19] is a 5G-enabled VANET hybrid message authentication scheme. It involves vehicles authenticating with Road Side Boxes to obtain local group signature private keys, using them to sign messages directly to other vehicles. Despite meeting specific security requirements, HDMA is less suitable for UAV scenarios due to its reliance on costly public cryptography and the absence of non-repudiation, a crucial security element for UAVs [2].

CBDDS [24] introduces a secure and revocable cache-based distributed data sharing scheme for privacy-preserving authentication between vehicles and Edge Servers (ES) in vehicular networks. In their approach, ES takes on roles of authentication and authorization, incorporating a token authentication mechanism and a multi-authority CP-ABE[1] algorithm for access control. However, their assumption of ES lacking resource limitations is not suitable for UAVs in our system model, and the computation overhead grows with the number of supported attributes.

The authors of [25] focused on UAV communication security in military zones, proposing two protocols: SP-D2GCS for communication between a drone and Ground Control Station, and SP-D2MD for communication between a drone and a monitoring drone, acting as a middleman to the ground station. Despite meeting some security requirements, their model relies on the monitoring drone transmitting all data. As a result, their protocols are not suitable for (1) resource-limited drones and (2) emergency networks when a connection to the ground station isn't available.

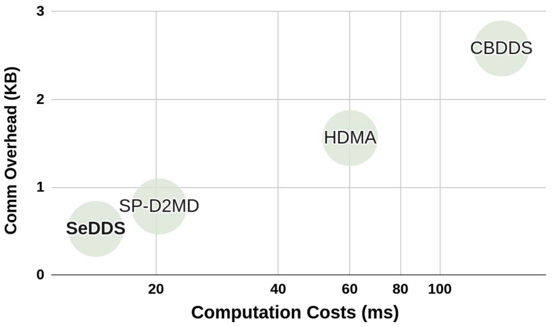


Figure 3. Direct Data Sharing Performance Comparison

In conclusion, SeDDS, as demonstrated in Table 4, reduces overall computation by 1.5 times and imposes a lighter communication load on UAVs and vehicles.

6. Security Analysis

In this section, we assess proposed protocols resilience within the defined threat model and discuss how to address compromised entities beyond this model considering real-world vulnerabilities of the entities.

6.1. Security Assessment of Protocols

- **Confidentiality and Integrity:** To safeguard exchanged data from unauthorized access, SeGDS encrypts file content with AES, and even if an adversary acquires a UAV's private key, the group leader can revoke victim's credential, preventing access to the session key shared via multicast encryption. In SeDDS, UAVs generate a secure symmetric encryption key through DHKE based on the DLP[2] assumption. Our protocols utilizes the certificateless signcryption [16] on all exchanged messages, ensuring confidentiality, data integrity, and unforgeability under the CDHP[3] and DLP assumptions.
- **High Availability** ensures system resilience to disruptions like DoS attacks. Our protocols guarantee service availability through UAV-friendly computation constraints, identifying and excluding entities causing delays, and enforced authentication on all message exchanges. Having timestamps on messages prevents replay attack.
- **Mutual Authentication** The AUSF plays a vital role in the 5G Core network, ensuring authentication for network entities among other responsibilities. This ensures the security of identity handling in our protocols. Additionally, mutual authentication occurs among all entities through signcryption of messages using CLGSC [16]. The scheme is resistant to forgery based on the DLP assumption. In both protocols, entities are required to verify the

[1] Cipher Policy Attribute Based Encryption

[2] Discrete Logarithm Problem

[3] Computational Diffie-Hellman Problem

TABLE 4. Comparative computation and communication costs analysis for Secure Direct Data Sharing Schemes

Scheme	Computation cost (ms)	Total bytes
HDMA [19]	$6T_e + 3T_{RSA_E} + 4T_{RSA_D} + 2T_{RSA_V} + T_{AES_E} + T_{AES_D}$ = 60.14	1560
CBDDS [24]	$15T_e + 13T_{pb} + 9T_{sm} + 2T_{RSA_G} + 2T_{RSA_V} + T_{AES_D}$= 141.83	2580
SP-D2MD [25]	$4T_e + 6T_m + 2T_{AES_E} + 2T_{AES_D}$ = 20.36	781
SeDDS	$2T_e + 10T_m + T_{AES_E} + T_{AES_D}$ = **14.20**	508

TABLE 5. Security Comparison in Direct and Group Data Sharing Schemes.

Security Requirements	HDMA [19]	CBDDS [24]	SP-D2MD [25]	Cui et al. [22]	Tan et al. [23]	**SeDDS**	**SeGDS**
Confidentiality and Integrity	✓	✓	✓	✓	✓	✓	✓
High Availability	✗	✗	✓	✗	✗	✓	✓
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓
Non-Repudiation	✗	✓	✗	✓	✓	✓	✓
Content-agnostic	✓	✗	✓	✗	✗	✓	✓
Support Offline Connection	✗	✗	✗	✗	✗	✓	✗
Support Group Data Sharing	✗	✗	✗	✓	✓	✗	✓
Support Vehicle/UAV Revocation	✗	✓	✗	✗	✓	✓	✓
Resist Collusion attack	✓	✓	✗	✗	✓	✓	✓
Resist Free-ridding attack	✗	✗	✗	✗	✗	✓	✓

sender's signature at each step before advancing further.

- **Non-repudiation** In UAV aided data sharing, it is crucial to ensure actions cannot be denied [2]. Signatures from the content service provider and UAVs prevent forgery and denial attacks, ensuring detectability and non-repudiation. The ID and timestamp on each message reveal participation details. In SeGDS, any attempt to share tampered data is easily detected. In SeDDS, malicious UAV_j sharing tampered data with VID_i requires a valid Ack message from VID_i to prove an honest data exchange act. This Ack message contains $P_i \oplus (C')$ since AUSF uses the original data M from CSP to verify the signature. Unless UAV_j forges VID_i's signature, it cannot deny malicious behavior. VID_i cannot create a false report against UAV_j as it requires forging the UAV_j signature.
- **Content-agnostic** In UAV-assisted networks, the protocol's adaptability to diverse data types is crucial for applications like emergency networks [6] or base station traffic offloading. Unlike some approaches relying on contextual data, our protocols stay practical for real-world scenarios. Data selection in our protocols is directed by the RSU or vehicles, eliminating the dependency on historical data or static distributed storage systems.
- **Support Offline Device-to-device (D2D) communication** in unlicensed spectrum enhances energy efficiency, boosts data rates, reduces link latency, and allows devices to utilize interfaces like Bluetooth or Wi-Fi Direct [13]. Given the critical applications relying on this communication, such as public safety, its security is paramount, and, to the best of our knowledge, although there's D2D protocols with intervention of base station [19]-[24], there lacks a secure outbound autonomous D2D authentication and message exchange protocol except the proposed SeDDS scheme.
- **Support Group Data Sharing** SeGDS achieves lightweight overhead as group size increases, ensuring efficient collaboration for tasks. Fig 2 illustrates this effectiveness, maintaining support for mutual authentication, message integrity, and non-repudiation through strategic task splitting, preventing the need for full content sharing between the service provider and UAVs.
- **Support Vehicle/UAV revocation** We utilize certificateless public key cryptography (CLPKC) with blacklist-based revocation, where entities private key stems from contributions by both the KGC (Key Generator Center, here AUSF) and the entity itself. The KGC, while unaware of the entities private key, can authenticate its public key. In proposed protocols, if the malicious behavior of a UAV or vehicles exceeds a predefined threshold during protocol execution, its ID is blacklisted, preventing further service use. Note that CLPKC doesn't require certificate revocation on the remaining devices.
- **Resist Collusion attack** A collusion attack involves authorized but malicious UAVs collaborating to provide malicious services to authorized entities. In SeGDS, there are two scenarios of collusion attacks. (1) A group of malicious UAVs colluding with a legitimate group leader (RSU) to obtain session keys of other groups without participating in the protocol. This is prevented as the data encryption key is unique per group session and generated by the RSU and service provider through a Diffie-Hellman protocol. (2) A group of malicious UAVs colluding to share tampered data with benign UAVs is detected, as the service provider signs every file segment with a proper timestamp before sharing with UAVs.
- **Resist Free-riding Attack** Free-riding attacks involve attempting to receive data without participating or providing compensation. In SeGDS, detection of non-participating UAVs occurs during the data consolidation phase. This detection enables the RSU to prevent malicious UAVs from accessing the session key, as they are excluded from the multicast encryption scheme. In SeDDS, a VID_i attempting to receive data without acknowledging the recipient of the service faces two choices. They can either refrain from sending the key hint request

in step 3, rendering the encrypted data unusable, or they may try to create a fake report against UAV_j by forging UAV_j's signature. However, this latter option is impractical under the Discrete Logarithm Problem (DLP) assumption.

6.2. Further Analysis: Compromised RSUs

RSUs are vulnerable to compromise due to their physical accessibility. Here, we discuss mitigation strategies to address compromised RSUs in SeGDS.

- **Resist Message Fabrication** If a compromised RSU attempts to modify packet data received from the CSP while sharing with vehicles, it will be detectable by the vehicles since the CSP signs every file segment (step 3 of Co-op download phase) before sending to UAVs. Therefore, the RSU would need to forge the CSP signature, which is not feasible under the DLP assumption.
- **Mitigate DoS Attacks against UAVs** A compromised RSU may attempt to drain UAVs' energy, making them inaccessible due to their limited resources. While the RSU cannot fabricate messages, it can initiate fake data download sessions with large files, depleting UAVs' battery or storage. To counter this, we propose implementing a hardware file size limit on UAVs to reject large file downloads. This trade-off aligns with our goal of providing on-demand data sharing capability for public safety. Additionally, we plan to address this challenge in future work by monitoring the group leader's (e.g., RSU) behavior via designing a decentralized peer-to-peer mechanism for SeGDS, enabling UAVs to collectively execute the protocol even without RSU presence.
- **Support Zero Trust** In the defined threat model, RSUs are considered honest entities. However, to ensure the same level of security against honest-but-curious or malicious RSUs, we can adopt lightweight zero trust protocols like [26], wherein RSU would not be able to learn about the file contents due to the enforced access control policies.

In conclusion, the proposed protocols not only meet the established security requirements but also offer a robust array of security features compared to existing works, as delineated in Table 5.

7. Energy Efficiency

Ensuring both security and energy efficiency is critical in UAV-assisted networks. Here, we discuss how our proposed protocols achieve energy efficiency and outline our future research directions. Energy efficiency methods in UAV communication can be categorized into four groups [27]:

1) Designing lightweight communication protocols
2) Optimizing resource allocation
3) Enhancing trajectory planning
4) Integrating energy harvesting methods

Regarding (1), our protocols meet essential security requirements (as detailed in Sec. 6) while minimizing communication and computation burdens on devices (as measured in Sec. 5), achieving a reduction of approximately 1.5-2.5x. This is accomplished through the use of symmetric encryption and certificateless cryptography.

Approaches in (2) and (3) lie beyond our current expertise. However, studies suggest the potential of reconfigurable intelligent surfaces (RIS) to extend coverage by adapting to channel dynamics in drone communications [28]. Additionally, adopting technologies such as software-defined networking (SDN) and network function virtualization (NFV) has shown promise in UAV networks for resource management and scalability [2].

Regarding sustainable energy sources (4), a hybrid solar-RF[4] energy harvesting system presents a viable solution, enabling UAVs to sustain day and night flights.

In future work, we aim to evaluate the total energy consumption of our protocols on the Pixhawk platform [29], measuring concrete energy efficiency achieved in the categories explained above.

8. Related Work

While prior research explores UAV communication using various networking paradigm and blockchain consensus [30]- [31], our paper emphasizes securing data communication in UAV-assisted networks through authentication, key agreement, and data exchange protocols.

8.1. Authentication and Key Agreement

In the domain of Internet of Vehicles (IoV), [32] proposes a novel authenticated key management scheme renowned for its security and efficiency. This scheme incorporates certificateless group authentication, a notable feature aimed at mitigating the burden of public key overhead on devices. Transitioning from this approach, [33] addresses the distinct challenges posed by UAV-assisted Vehicular Ad-hoc Networks (VANETs). Here, they introduce a lightweight two-factor Authentication and Key Agreement (AKA) scheme based on chaotic maps, tailored to the unique characteristics of UAV deployments within VANETs.

Moreover, as the integration of unmanned aerial vehicles (UAVs) in VANETs becomes increasingly prevalent, optimizing resource utilization becomes paramount. To this end, [34] contributes an innovative drone-assisted anonymous AKA framework, designed specifically for 5G VANETs. Leveraging the Real-Or-Random (ROR) model, this framework achieves a delicate balance between security and computational overhead, making it particularly well-suited for UAVs operating within VANET environments. This transition underscores the evolving landscape of authentication and key agreement protocols in the context of UAV-assisted VANETs.

8.2. Secure Data sharing

In the context of UAVs, where secure data sharing remains a relatively new domain, insights gained from analogous networks like Device-to-Device (D2D) communications and Vehicular Ad-hoc Networks (VANETs).

[4] Solar-Radio Frequency

[35] proposes a secure data sharing scheme within the framework of 5G-enabled mobile devices, facilitated by base stations for connection establishment, while data transmission occurs directly between devices. Noteworthy is the introduction of an incentive mechanism aimed at fostering user participation, coupled with robust measures to track and deter malicious behavior, thereby ensuring service availability and thwarting free-riding attacks.

Transitioning to the domain of 5G-enabled vehicular networks, [15] presents a secure content-sharing approach. However, its reliance on a Trusted Authority (TA) to manage buffers for content tracking raises practical concerns, particularly in dynamic content sharing scenarios and emergency situations where TA availability for vehicle selection may be limited.

Meanwhile, [36] introduces a rapid authentication and data distribution protocol within the framework of 3GPP 5G networks. Here, a collective of narrowband Internet of Things (IoT) terminals achieves concurrent access authentication and data transmission, catering to the growing demand for efficient data dissemination in IoT environments.

In response to the imperative for a secure video reporting scheme, [37] outlines a novel approach wherein edge nodes assume the responsibility of message verification and classification. This methodology expedites report analysis and resolution of duplicates, addressing critical requirements for efficient and reliable video reporting systems. Similarly, [38] reveals security vulnerabilities in vehicular video reporting services such as replay, message fabrication and DoS attacks. Authors proposed strategies to mitigate such attacks in VANETs.

9. Conclusion

In conclusion, this paper addresses the pressing demands for scalability, high availability, and security in VANETs through the introduction of two protocols, SeDDS and SeGDS. SeDDS enables secure direct data sharing among devices in an out-of-band autonomous communication setting, eliminating the need for a trusted party or presuming trust among entities. On the other hand, SeGDS presents a collaborative data sharing scheme, meeting security requirements for swarm UAVs while minimizing computation and communication costs. The meticulous evaluation of these protocols, demonstrated through comparative analyses, underscores their superiority in both security and efficiency over existing models. As we navigate the evolving landscape of 6G, these protocols provide a transformative pathway toward unlocking the full potential of drone-assisted communication. Future work will focus on enhancing resistance against a broader range of attacks, particularly those targeting entities hardware.

Appendix

Certificateless Generalized Signcryption (CLGSC) scheme. Generalized signcryption is a cryptographic primitive that not only can obtain encryption and signature in a single operation, but also provide encryption or signature model alone when needed. Zhang et al. [16] proposed an lightweight CLGSC scheme with low computation overhead which is composed of four algorithms defined as follows:

*Setup(k).*The KGC generates two primes p and q, with the chosen security parameter k, where $q|p-1$ and a cyclic group G with prime order q and a generator of P. The KGC selects random number $x_N \in Z_q^*$ as the master private key, then, computes $X_N = x_N P$ as the public key. Moreover, the KGC chooses three secure hash functions: $H_1 : \{0,1\}^* \times G \times G \times G \rightarrow Z_q^*$, $H_2 : Z_q^* \times Z_q^* \rightarrow Z_q^*$, $H_3 : Z_q^* \times Z_q^* \rightarrow \{0,1\}^*$. Define an index function $f(ID)$ such that, $f(ID) = 0$ if ID = $\emptyset$, otherwise $f(ID) = 1$. The system parameters is published as $params = (p, q, P, X_N, H_1, H_2, H_3)$.

KeyGen(ID_i). This algorithm is performed between the user ID_i and KGC interactively.

- The user ID_i randomly selects $x_i \in Z_q^*$ as part of its private key and computes $X_i = x_i P$ as its partial public key and sends (ID_i, X_i) to KGC.
- The KGC randomly selects $y_i \in Z_q^*$ and computes $Y_i = y_i P$, $z_i = y_i + x_N H_1(ID_i, Y_i, X_i, X_N)$ for the user with partial public key X_i. The KGC sends the partial private key z_i of user ID_i through a secure channel and its public key (X_i, Y_i) is stored in the public tree by the KGC.[5]

*CLGSC(ID_A, ID_B, m).*The sender ID_A to perform a signcryption (signature or encryption) of the message m for the receiver ID_B goes through following steps:

- Computes $f(ID_A), f(ID_B)$;
- ID_A randomly selects $r \in Z_q^*$, and computes $h_1 = H_1(ID_B, Y_B, X_B, X_N)$;
- Computes $f_1 = rP, f_2 = rf(ID_A)/(x_A + z_A + f_3), f_3 = H_2(f_1, ID_A, m)$;
- Computes $m' = (H_3(v_1, v_2)f(ID_B)) \oplus m$, in which $v_1 = rX_B, v_2 = r(Y_B + h_1 X_N)$;
- Returns $\mu = (f_1, f_2, f_3, m')$ as the ciphertext.

UCLGSC(ID_A, ID_B, μ). The receiver ID_B can decrypt and verify μ as follows:

- Computes $f(ID_A), f(ID_B), h_1' = H_1(ID_A, Y_A, X_A, X_N)$;
- Computes $v_1' = x_B f_1, v_2' = z_B f_1, m = (H_3(v_1', v_2')f(ID_B)) \oplus m'$;
- Checks $H_2(f_2(X_A + Y_A + h_1' X_N + f_3 P), ID_A, m) = f_3$ for signature verification and $H_2(f_1, ID_A, m) = f_3$ for the encryption mode. If the equation holds, the message is accepted.

References

[1] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas *et al.*, "On the road to 6g: Visions, requirements, key technologies and testbeds," *IEEE Communications Surveys & Tutorials*, 2023.

[2] M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Żywiołek, and I. Ullah, "Swarm of uavs for network management in 6g: A technical review," *IEEE Transactions on Network and Service Management*, 2022.

[5] The user ID_i can verify the validity of the partial private key by checking whether $Y_i + H_1(ID_i, Y_i, X_i, X_N)X_N = z_i P$.

[3] N. Lin, Y. Liu, L. Zhao, D. O. Wu, and Y. Wang, "An adaptive uav deployment scheme for emergency networking," *IEEE Transactions on Wireless Communications*, vol. 21, no. 4, pp. 2383–2398, 2021.

[4] O. S. Oubbati, N. Chaib, A. Lakas, P. Lorenz, and A. Rachedi, "Uav-assisted supporting services connectivity in urban vanets," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3944–3951, 2019.

[5] R. Zhang, R. Lu, X. Cheng, N. Wang, and L. Yang, "A uav-enabled data dissemination protocol with proactive caching and file sharing in v2x networks," *IEEE Transactions on Communications*, vol. 69, no. 6, pp. 3930–3942, 2021.

[6] Y. Gao, J. Cao, P. Wang, J. Yin, M. He, M. Zhao, M. Peng, S. Hu, Y. Sun, J. Wang *et al.*, "Intelligent uav based flexible 5g emergency networks: Field trial and system level results," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 138–143.

[7] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "Sok: Security and privacy in the age of commercial drones," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1434–1451.

[8] D. Koisser, R. Mitev, M. Chilese, and A.-R. Sadeghi, "Don't shoot the messenger: Localization prevention of satellite internet users," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2024, pp. 66–66.

[9] M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk, and H. Song, "A systematic survey: security threats to uav-aided iot applications, taxonomy, current challenges and requirements with future research directions," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1437–1455, 2022.

[10] M. O. Ozmen, H. Farrukh, H. Kim, A. Bianchi, and Z. B. Celik, "Short: Rethinking secure pairing in drone swarms," *"Symposium on Vehicles Security and Privacy (VehicleSec)"*, 2023.

[11] A. V. Shvetsov, S. H. Alsamhi, A. Hawbani, S. Kumar, S. Srivastava, S. Agarwal, N. S. Rajput, A. A. Alammari, and F. Nashwan, "Federated learning meets intelligence reflection surface in drones for enabling 6g networks: challenges and opportunities," *IEEE Access*, 2023.

[12] 3rd Generation partnership project (3GPP), "5g; security architecture and procedures for 5g system (3gpp ts 33.501 version 17.5.0 release 17)," Tech. Rep., 2022.

[13] M. S. M. Gismalla, A. I. Azmi, M. R. B. Salim, M. F. L. Abdullah, F. Iqbal, W. A. Mabrouk, M. B. Othman, A. Y. Ashyap, and A. S. M. Supa'at, "Survey on device to device (d2d) communication for 5gb/6g networks: Concept, applications, challenges, and future directions," *IEEE Access*, vol. 10, pp. 30 792–30 821, 2022.

[14] S. Zhang, H. Zhang, and L. Song, "Beyond d2d: Full dimension uav-to-everything communications in 6g," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6592–6602, 2020.

[15] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5g-enabled vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1247–1259, 2020.

[16] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2016.

[17] S. H. Islam, M. K. Khan, and A. M. Al-Khouri, "Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing," *Security and communication networks*, vol. 8, no. 13, pp. 2214–2231, 2015.

[18] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[19] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "Hdma: Hybrid d2d message authentication scheme for 5g-enabled vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5071–5080, 2020.

[20] "Miracl library," *Available: https://github.com/miracl/MIRACL.*

[21] "Pairing-based cryptography library," *Available: https://crypto.stanford.edu/pbc/.*

[22] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in vanets-an efficient and privacy-preserving cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[23] H. Tan and I. Chung, "Rsu-aided remote v2v message dissemination employing secure group association for uav-assisted vanets," *Electronics*, vol. 10, no. 5, p. 548, 2021.

[24] J. Zhang, X. Liu, J. Cui, H. Zhong, L. Wei, I. Bolodurina, and D. He, "Cbdds: Secure and revocable cache-based distributed data sharing for vehicular networks," *IEEE Transactions on Mobile Computing*, 2023.

[25] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, "Drone secure communication protocol for future sensitive applications in military zone," *Sensors*, vol. 21, no. 6, p. 2057, 2021.

[26] A. Mohseni Ejiyeh, "Real-time lightweight cloud-based access control for wearable iot devices: A zero trust protocol," in *Proceedings of the First International Workshop on Security and Privacy of Sensing Systems*, 2023, pp. 22–29.

[27] H. Jin, X. Jin, Y. Zhou, P. Guo, J. Ren, J. Yao, and S. Zhang, "A survey of energy efficient methods for uav communication," *Vehicular Communications*, vol. 41, p. 100594, 2023.

[28] N. Abuzainab, M. Alrabeiah, A. Alkhateeb, and Y. E. Sagduyu, "Deep learning for thz drones with flying intelligent surfaces: Beam and handoff prediction," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2021, pp. 1–6.

[29] Available online: https://pixhawk.org/.

[30] H. Luo, Y. Wu, G. Sun, H. Yu, and M. Guizani, "Escm: an efficient and secure communication mechanism for uav networks," *IEEE Transactions on Network and Service Management*, 2024.

[31] J. Wang, Z. Jiao, J. Chen, X. Hou, T. Yang, and D. Lan, "Blockchain-aided secure access control for uav computing networks," *IEEE Transactions on Network Science and Engineering*, 2023.

[32] H. Tan, W. Zheng, and P. Vijayakumar, "Secure and efficient authenticated key management scheme for uav-assisted infrastructure-less iovs," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[33] J. Cui, X. Liu, H. Zhong, J. Zhang, L. Wei, I. Bolodurina, and D. He, "A practical and provably secure authentication and key agreement scheme for uav-assisted vanets for emergency rescue," *IEEE Transactions on Network Science and Engineering*, 2023.

[34] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5g/b5g vehicular ad-hoc networks," *IEEE transactions on network science and engineering*, vol. 8, no. 4, pp. 2982–2994, 2020.

[35] A. Mohseni-Ejiyeh, M. Ashouri-Talouki, and M. Mahdavi, "An incentive-aware lightweight secure data sharing scheme for d2d communication in 5g cellular networks." *ISeCure*, vol. 10, no. 1, 2018.

[36] J. Cao, P. Yu, M. Ma, and W. Gao, "Fast authentication and data transfer scheme for massive nb-iot devices in 3gpp 5g network," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1561–1575, 2018.

[37] H. Zhong, L. Wang, J. Cui, J. Zhang, and I. Bolodurina, "Secure edge computing-assisted video reporting service in 5g-enabled vehicular networks," *IEEE Transactions on Information Forensics and Security*, 2023.

[38] A. Mohseni-Ejiyeh and M. Ashouri-Talouki, "Sevr+: Secure and privacy-aware cloud-assisted video reporting service for 5g vehicular networks," in *2017 Iranian conference on electrical engineering (ICEE)*. IEEE, 2017, pp. 2159–2164.