

# liteGAP: Lightweight Group Authentication Protocol for Internet of Drones Systems

Cong Pu <sup>1</sup>, Member, IEEE, Clare Warner, Kim-Kwang Raymond Choo <sup>2</sup>, Senior Member, IEEE, Sunho Lim <sup>3</sup>, Senior Member, IEEE, and Imtiaz Ahmed <sup>4</sup>, Member, IEEE

**Abstract**—Over the past few years, the synergic usage of unmanned aerial vehicles (later drones) and Internet of Things (IoT) has successfully transformed into the Internet of Drones (IoD) paradigm, where the data of interest is gathered and delivered to the Zone Service Provider (ZSP) by drones for substantial additional analysis. Considering the sensitivity of collected information and the impact of information disclosure, information privacy and security issues should be resolved properly so that the maximum potential of IoD can be realized in the increasingly complex cyber threat environment. Ideally, an authentication and key agreement protocol can be adopted to establish secure communications between drones and the ZSP in an insecure environment. Nevertheless, a large group of drones authenticating with the ZSP simultaneously will lead to a severe authentication signaling congestion, which inevitably degrades the quality of service (QoS) of IoD systems. To properly address the above-mentioned issues, a lightweight group authentication protocol, called *liteGAP*, is proposed in this paper. *liteGAP* can achieve the authenticated key establishment between a group of drones and the ZSP concurrently in the IoD environment using lightweight operations such as hash function, bitwise XOR, and physical unclonable function (PUF). We verify *liteGAP* using AVISPA (a tool for the automatic verification of security protocols) and conduct formal and informal security analysis, proving that *liteGAP* meets all pre-defined security requirements and withstand various potential cyber attacks. Moreover, we develop an experimental framework and conduct extensive experiments on *liteGAP* and two benchmark schemes (e.g., GASE and rampIoD). Experimental findings show that *liteGAP* outperforms its counterparts in terms of computational cost as well as communication overhead.

**Index Terms**—Information privacy and security, Internet of Drones, signaling congestion, group authentication.

## I. INTRODUCTION

IN THE third decade of the 21st century, drones have entered a new realm owing to today's technological advances in

Manuscript received 16 April 2023; revised 1 July 2023; accepted 16 November 2023. The review of this article was coordinated by Dr. Ming Li. (Corresponding author: Cong Pu.)

Cong Pu and Clare Warner are with the Department of Computer Science, Oklahoma State University, Stillwater, OK 74078 USA (e-mail: cong.pu@outlook.com; clawarn@okstate.edu).

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: raymond.choo@fulbrightmail.org).

Sunho Lim is with the Department of Computer Science, Texas Tech University, Lubbock, TX 79409 USA (e-mail: sunho.lim@ttu.edu).

Imtiaz Ahmed is with the Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059 USA (e-mail: imtiaz.ahmed@howard.edu).

Digital Object Identifier 10.1109/TVT.2023.3335839

robotics automation and control, and their applications have increased rapidly in various fields. For example, on March 29, 2021, 3,281 drones lighted up night sky in Shanghai and formed into the emblem of luxury vehicle brand Genesis, making a Guinness World Records title for the most drones airborne simultaneously. To fight against coronavirus and save lives across the world, drones have been widely used by healthcare providers and biopharmaceutical companies to deliver medicines and vaccines to hard-to-reach places. Pfizer Inc. announced that Zipline (a global instant logistics company) has successfully completed the first COVID-19 vaccine drone delivery in Ghana on November 11, 2021. Drone technology also has the potential to bring huge economic and societal benefits. According to the April 2021 “Commercial Drone Market” report published by Grand View Research [1], the drone industry is booming and its market value is expected to be worth \$47.38 billion globally by 2029. With the innovative developments in materials science, wireless communication, as well as computing and storage, it is predictable that drone technology will transform the way we work and live in the near future.

As drones are becoming more commonplace and have widespread adoption, many attempts have been made to revolutionize the traditional Internet of Things (IoT) by embracing drones, and build a promising air-ground integrated communication architecture, which is known as the Internet of Drones (IoD) [2]. The IoD paradigm partitions airspace into zones, each of which is coordinated and administered by one or more Zone Service Providers (ZSPs). The primary function of ZSPs is to allow drones to connect to a wired network. Typically, a plethora of drones are deployed to gather task-related information in the zone and deliver them to the ZSP for further information mining and analysis. With the growing prevalence of drones, numerous real-world applications have quickly emerged around the IoD, ranging from law enforcement surveillance to construction surveying and inspection. In these emerging applications, drones can often make the trip faster or accomplish a task more efficiently with less risk. A telling example is that drones can survey dangerous sites, sparing employees from exposure to threats like noxious gas or shaky structures.

### A. Motivation

The transformative power of the IoD has been demonstrated in civilian applications during the coronavirus pandemic. However, to unleash the full potential of the IoD, several issues need to

be properly addressed. First, the data collected by drones might contain sensitive attributes (i.e., facial recognition drones collect and store very sensitive and personally identifiable information), thus, the communications between drones and the ZSP over an open network need to be protected from unauthorized access [3]. Specifically, before exchanging sensitive information, drones and the ZSP need to perform identity verification and reach an agreement on the session keys. Second, as a result of drones' scarce resources, however, full-fledged security solutions (e.g., FPGA-based RSA and AES) cannot be directly applied [4]. We also have to be cognizant of the fact that drones' capabilities and functionalities must not be affected by the security schemes, e.g., heavyweight security schemes consume a significant amount of energy, shortening the lifespan of drones. Third, if a large group of drones communicates with the ZSP for authentication and key establishment simultaneously, a severe authentication signaling congestion will occur at the ZSP [5]. As a result, drones might be faced with authentication failure or even suffer denial of service, and the overall quality of service (QoS) is adversely affected.

### B. Contribution

Based upon the above discussion, this paper proposes a security solution that allows a large group of drones to communicate with the ZSP simultaneously and securely over an open network. We also perform an in-depth security analysis and conduct extensive experiments to evaluate the proposed approach. In short, our main contributions are listed as follows:

- We propose a lightweight group authentication protocol, called *liteGAP*, for IoD systems. *liteGAP* can achieve the authenticated key establishment between a group of drones and the ZSP concurrently using lightweight operations such as hash function, bitwise XOR, and physical unclonable function (PUF).
- We verify *liteGAP* using AVISPA (a tool for the automatic verification of security protocols) [6] as well as conduct formal and informal security analysis, proving that *liteGAP* meets all pre-defined security requirements and withstand various potential cyber attacks.
- We develop an experimental framework and conduct extensive experiments on *liteGAP* and two benchmark schemes, GASE [7] and rampIoD [8], for performance evaluation.

The experimental findings demonstrate that *liteGAP* can meet all security requirements while achieving lower computational cost and communication overhead.

### C. Novelty

Our work is novel in the matter of three aspects: investigating emergent IoD architecture; developing unprecedented group authentication protocol; and adopting resource-friendly operations. First, we devote our efforts to the IoD paradigm which is arguably one of the most important subjects for scientific investigation within many technical communities and commercial companies. Our thorough analysis of IoD architecture will serve as a theoretical foundation for understanding its unique security and privacy challenges and requirements. Second, we propose a group authentication protocol for IoD

systems. Over the last couple of years, several authentication mechanisms have been proposed to protect the IoD communications. However, what has been lacking in the current theory is a secure and lightweight group authentication protocol that adopts resource-friendly computing operations to achieve the security and efficiency requirements concurrently for drone communications in the IoD environment. Third, the proposed group authentication protocol is realized with three resource-friendly techniques: hash function, bitwise XOR, and PUF. Compared to other heavyweight techniques (i.e., elliptic curve cryptography, bilinear pairings, etc.) which are used for resource-constrained communication systems, our solution has less computational and storage overhead while meeting the required security requirements.

### D. Paper Organization

The rest of the paper is organized as follows. Section II presents and analyzes the state of the art. The background information of associated technique is provided in Section III. We describe network and adversary models, as well as security requirements in Section IV. *liteGAP* is proposed in Section V. Section VI and VII are devoted to security verification and analysis, and experimental study, respectively. Lastly, the paper is concluded in Section VIII.

## II. RELATED WORK

During recent years, some researchers have investigated authenticated key agreement mechanisms so that the entities of IoD systems are able to exchange information securely in an untrustworthy environment. In [9], the authors first expose real weaknesses (i.e., single point of failure and lack of inter-domain authentication) of centralized IoD authentication systems. Then, they design a blockchain assisted cross-domain authentication scheme to protect drone communications in the IoD environment, where a drone's federated identity is created using a threshold signature scheme. Moreover, drones from different domains are able to verify each other's identities and set up secure session keys with the assistance of smart contract. The experimental study demonstrates that the proposed scheme has promising performance from the efficiency and effectiveness point of view. However, the authentication signaling congestion problem existing in the intra-domain did not get authors' attention at all. In [8], an authentication scheme based upon elliptic curve cryptosystem and hash algorithm is developed for IoD networks. Before the drone and the user share any critical information over an insecure channel, their identifications are required to be verified first, and then they can reach an agreement on the session key. One striking feature of their approach is the privacy guarantee: the user's and drone's identity information are not disclosed during the authentication process. The proposed scheme delivers better performance along with advanced security features, nevertheless, it only allows the user to authenticate with one drone at a time. When the user needs to establish mutual authentication with a large number of drones simultaneously for the task of interest, a non-negligible amount of communication overhead can be expected because the same

authentication process has to be repeated a sufficient number of times. The authors in [10] design a group handover mechanism for 5G-enabled vehicle-to-Everything networks, where the vehicle leader performs mutual authentication with the core network on behalf of other vehicles. However, vehicles are assumed to have unlimited resources to perform cryptographic operations, which is not the case in the IoD environment.

Another area of research has been on the development of security solutions for the IoT networks. In [11], the authors investigate the device-to-device (D2D) communication and its security threats in the 5G-enabled IoT setting. To protect IoT devices (e.g., drones) from malicious attacks, a 5G D2D ProSe standard compatible authentication mechanism is proposed. Precisely, the leader drone first registers with the core network, and then broadcasts a proxy signature so that it can achieve mutual authentication with other adjacent drones. After that, the leader drone serves as a relay point between the backbone network and the drone swarm for the exchange of critical data. Regrettably, acting as the relay node will turn the leader drone into a single point of failure (SPoF), which makes the entire network vulnerable to cyber attacks. In [12], a federated learning (FL) based drone authentication model is designed for drone-enabled IoT networks, where the deep neural network integrated with stochastic gradient descent optimization is performed on drones locally for authentication. In addition, to secure critical parameters, the secure aggregation mechanism and homomorphic encryption are adopted. Unfortunately, the major drawback is that the deep learning model is energy intensive to the resource-constrained drones.

In [13], the authors propose a group signature mechanism for blockchain-enabled mobile-edge computing systems. If the new block contains a valid group signature created through the BLS aggregate signature algorithm, it is regarded as a legal block. In addition, they propose an authentication scheme for mobile device users to relocate between different groups in the network. The basic idea is to store the authentication credentials in the blockchain so that mobile device users can access them in the blockchain for authentication. In [14], a certificate-free authenticated key agreement mechanism is developed for 5G D2D networks, where the public key and elliptic curve cryptosystems are adopted to realize the authentication. Moreover, a digital signature is created to protect D2D group communications from internal attackers. The authors in [15] develop a secure message exchange protocol for IoT networks. Through the secure protocol, IoT devices and untrustworthy edge servers are able to exchange information freely. In [16], the authors point out that sequentially authenticating RFID tags will generate heavy communication workloads. To resolve this issue, a security solution that can achieve group authentication of RFID tags is developed. If a group of RFID tags respond to the authentication requests simultaneously, a confirmable bit-collision pattern will be generated, indicating that the responses of authentication requests come from the entire group. However, in all the abovementioned studies, the authors did not take into account mobility, thus, their approaches are unable to be employed for IoD systems.

In [17], the authors propose an in-network caching for fast content delivery in Vehicle-to-Grid (V2G) networks, where each vehicle will evaluate the reputation score of content provider

before retrieving their content. In addition, the blockchain technique is adopted to securely store the reputation value and incentives-related transactions. In [18], the authors present blockchain and UAV-enabled edge computing based energy trading services for the V2G environment. In their approach, the electric vehicle will select a charging station which is close to its moving path with the assistance of edge node. The investigated topics in [17], [18] are urgent, but are not duplicative of what is being investigated in this paper. Given the expected impact of the research outcomes, the proposed research is expected to amplify the authors' productivity in the V2G domain, as well as be complementary to what is being done elsewhere and, more likely, to be synergistic. In summary, many researchers spent effort on the security issues of IoD systems and developed various authentication mechanisms. However, they did not give much attention to a lightweight group authentication protocol based upon lightweight operations to protect communications between a group of drones and the ZSP in the IoD environment.

### III. PRELIMINARY: PHYSICAL UNCLONABLE FUNCTION

Physical unclonable functions (PUFs) are universally utilized as a hardware-specific security primitive to offer cryptographic services for electronic devices [19]. The physical structure of PUF is formed in the process of manufacturing. Since it is inevitable for each integrated circuit to have slight physical differences from the manufacturing process, the PUF is believed to be impossible to replicate or clone. Thanks to its unique features, the PUF is generally considered to be the identification of an electronic device, which is analogous to a person's social security number.

Typically, the PUF is fed with an input, termed *challenge*, and generates an output, named *response*. The combination of challenge and response goes by the name challenge-response pair (CRP). A single PUF always responds to the same challenge equivalently (i.e., the same response is produced), and two distinct PUF instances should respond to the same unbiased challenges differently (i.e., the different responses are produced). According to [20], the PUF can be represented as a mathematical function, denoted as  $res = F_{puf}(che)$ , where *che* and *res* indicate PUF's challenge and response, respectively.

In noisy environments, the identical challenges fed to the PUF might not be able to get the same responses [20]. In other words, the PUF is sensitive to external environment changes/noise, thus, the secret data of cryptographic operations might not be regenerated by the PUF. To resolve this important issue, error correction code (ECC) and fuzzy extractor can be integrated with the PUF. First, we define an algorithm to generate the response, *rGen*. The *rGen* algorithm will output a set  $\{res, S\}$ . Here, *res* is the CRP response, which is the value to be regenerated by the PUF. *S* is a helper string which is fed into the PUF to regenerate the CRP response *res*. The error correction code (ECC) [21] is adopted to eliminate up to  $x$  bit errors in the CRP response *res*.

We also design a response restore algorithm, denoted as *rRes*. The main purpose of *rRes* is to allow the PUF to restore the CRP response *res* with the assistance of the helper string *S* and the error decoding algorithm  $D_{er}$ , even if the PUF produces an output  $O'$  that differs from the original output  $O$  by at most  $x$  bits.

**Algorithm 1:** Response Generation Algorithm  $rGen$ .**Input:** Modulus  $n$ ; Challenge  $che$ 


---

```

1 Function  $rGen(n, che)$  :
  /*  $\overset{\circledast}{\leftarrow}$  denotes sampling */
  /*  $\oplus$  denotes exclusive OR function */
  /*  $\mathbb{Z}_n$  denotes the set of remainders in
  arithmetic modulo  $n$  */
2  $O = F_{puf}(che)$ ;
3  $res \overset{\circledast}{\leftarrow} \mathbb{Z}_n$ ;
4  $S = O \oplus ECC(res)$ ;
5 return  $\{res, S\}$ ;

```

---

**Algorithm 2:** Response Restore Algorithm  $rRes$ .**Input:** Challenge  $che$ ; Helper string  $S$ 


---

```

1 Function  $rRes(che, S)$  :
2  $O' = F_{puf}(che)$ ;
3  $res = Der(S \oplus O')$ ;
4 return  $res$ ;

```

---

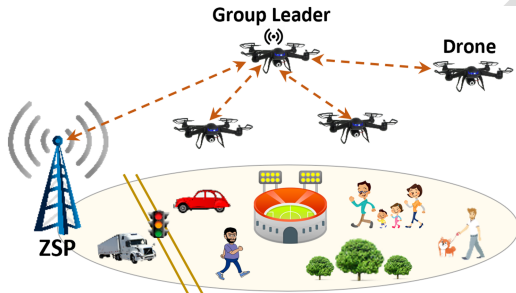


Fig. 1. Network model.

## IV. NETWORK AND ADVERSARY MODELS

## A. Network Model

In this paper, there are two major entities, ZSP and drones, which are shown in Fig. 1. It is assumed that every drone is furnished with a PUF, and has limited resources (e.g., battery energy). The focus of this paper is on the mutual authentication with privacy protection in the IoD environment, thus, we do not spend effort on the design and creation of real PUF. For simplicity, the PUF is simulated as a secure process integrated with fuzzy extractor method and error-correcting technique (see more details about the implementation of PUF in Section III). In addition, the ZSP is regarded as a trusted entity with no resource constraints.

Without loss of generality, we consider the scenario in which a large group of drones wants to exchange sensitive information with the ZSP. Since the data will be transmitted over an insecure communication channel, thus, drones need to authenticate and establish secure session keys with the ZSP before sharing any critical information. However, if a large group of drones sends their separate authentication request messages to the ZSP simultaneously, authentication signaling congestion might occur at the ZSP, which can cause authentication failure or even denial of service. Thus, an efficient and lightweight group authentication

protocol dedicated for resource-constrained drones is required for IoD systems.

## B. Adversary Model

The formalization of the adversary model is based on Dolev–Yao threat framework [22]. Thus, the adversary is believed to have boundless power so that it can control the communication network. In addition, the adversary can disguise itself as a legitimate entity of the network. This, in turn, means that the adversary has the ability to compromise the transmitted messages. In the IoD setting, it is difficult or impossible to protect drones physically. Thus, there is some chance that the drone is physically captured by the adversary [23]. However, if the adversary plans to fetch the secret data from the PUF, the physical characteristics of PUF will be compromised and the original CRP will be destroyed. To sum up, the primary goal of the adversary is to pretend to be a legitimate entity and communicate with the trusted ZSP or any legitimate drone, and then cause serious damage to the national interest, organizations or individuals.

## C. Security Requirements

According to the well-known security objectives of computing services [24], we outline the following security requirements to be satisfied by our approach *liteGAP*.

- **Group Authentication:** *liteGAP* must ensure the authenticity of a group of drones and the ZSP, that is, each is the entity that it claims to be. Additionally, *liteGAP* should not allow any adversary to disguise itself as a legitimate entity (drone or ZSP) for malicious purposes.
- **Group Session Key Establishment:** After successful group authentication, *liteGAP* must achieve an agreement on session keys between a group of drones and the ZSP. In addition, *liteGAP* must ensure that an adversary is unable to obtain intelligence from the captured session key.
- **Confidentiality:** After a secure session key is established, *liteGAP* must assure that confidential messages are securely shared between drones and the ZSP over an open network, and not made available or disclosed to unauthorized adversary.
- **Integrity:** *liteGAP* must perform the verification on the source of messages, and make sure that the messages are free from deliberate or inadvertent unauthorized manipulation or modification.
- **Anonymity:** *liteGAP* must use the pseudonyms of drones during the group authentication phase. Moreover, *liteGAP* must ensure that the real identities of drones are only known to the trusted ZSP, and an adversary cannot reveal drones' real identities via eavesdropping.
- **Secure Against Cyber Attacks:** *liteGAP* must be secure against well-known cyber attacks such as ZSP spoofing attack, replay attack, message modification attack, man-in-the-middle attack, drone capture attack, known session key attack, and drone impersonation attack.

TABLE I  
 NOTATIONS

Notation	Meaning
$ZID_s$	The identity of ZSP $Z_s$
$ID_i$	The real identity of drone $N_i$
$PID_i$	The pseudonym of drone $N_i$
$che_i$	Drone $N_i$ 's PUF challenge
$res_i$	Drone $N_i$ 's PUF response
$(che_i, res_i)$	Drone $N_i$ 's challenge-response pair (CRP)
$F_{puf}^i(\cdot)$	Drone $N_i$ 's PUF
$rGen(\cdot)$	PUF response generation algorithm
$rRes(\cdot)$	PUF response restore algorithm
$S$	Helper string
$n$	Modulus $n$
$H(\cdot)$	Hashing algorithm
$\oplus$	Bitwise XOR
$\parallel$	Concatenation operation
$T_j$	The $j$ th task or mission
$t$	Timestamp
$r_i^t$ and $r_s^t$	Nonce generated by drone $N_i$ and ZSP $Z_s$
$PR_s$	ZSP $Z_s$ 's private key
$GID_j$	Group identity for drones associated with $T_j$
$GT_j$	Group token for drones associated with $T_j$
$GK_j$	Group key for drones associated with $T_j$
$GL_j$	Group leader for $T_j$
$C(\cdot)$	Message authentication code (MAC) function
$M_{id}^k$	The message $k$ generated by entity $id$
$MAC_{id}^k$	The MAC of message $k$ generated by entity $id$
$MAC_j^*$	The aggregate MAC for $T_j$
$M_j^*$	The aggregate authentication request for $T_j$
$SK_{i,s}$	Secret session key between drone $N_i$ and ZSP $Z_s$

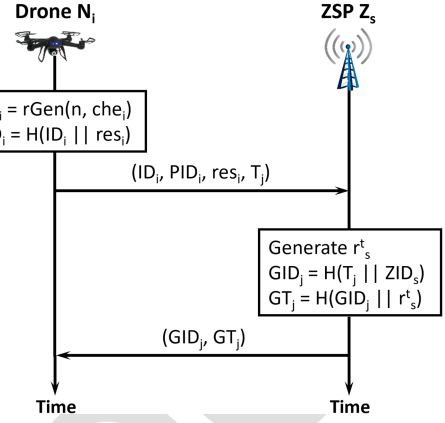


Fig. 2. Registration phase.

- 1)  $Z_s$  chooses its identity  $ZID_s$ , private key  $PR_s$ , and a hashing algorithm  $H(\cdot)$ .  $Z_s$  publishes  $(ZID_s, H(\cdot))$  while keeps  $PR_s$  securely.
- 2)  $N_i$  randomly chooses its real identity  $ID_i$  and PUF challenge  $che_i$ .  $N_i$  saves  $(ID_i, che_i)$  secretly.

### B. Registration Phase

In the registration phase, drone  $N_i$  registers with ZSP  $Z_s$  by submitting a registration request. Upon receiving the registration request from  $N_i$ ,  $Z_s$  generates the group authentication related information and share them with  $N_i$ . When the registration phase is over,  $Z_s$  will obtain  $N_i$ 's real identity, pseudonym, PUF challenge, and group authentication information, while  $N_i$  will receive its group authentication related information. Fig. 2 presents the registration process of *liteGAP*, and the key steps of registration process are explained below.

- 1)  $N_i$  feeds its PUF challenge  $che_i$  into response generation algorithm  $rGen(\cdot)$  and computes the corresponding PUF response  $res_i = rGen(n, che_i)$ .  $N_i$  also feeds its  $ID_i$  and  $res_i$  into the hashing algorithm to calculate the pseudonym  $PID_i = H(ID_i || res_i)$ . Here, the pseudonym of drone, rather than the real identity of drone, will be used for the communication with the group leader later to preserve the identity privacy of drone.
- 2)  $N_i$  sends a registration request containing  $(ID_i, PID_i, res_i, T_j)$  to  $Z_s$  via a secure channel (e.g., time-based OTP algorithm (TOTP) [25]).
- 3) After receiving the registration request from  $N_i$ ,  $Z_s$  generates a nonce  $r_s^t$ , and computes the group identity  $GID_j = H(T_j || ZID_s)$  and the group token  $GT_j = H(GID_j || r_s^t)$ . Note that this step is only executed when  $Z_s$  receives the first registration request for the task  $T_j$ .
- 4)  $Z_s$  stores  $(ID_i, PID_i, res_i, T_j, GID_j, GT_j)$  in the database, and sends  $(GID_j, GT_j)$  to  $N_i$  via a secure channel. Here,  $Z_s$  stores  $GID_j$  and  $GT_j$  so that it does not need to re-calculate them when the other drone registers for the same task  $T_j$ .
- 5)  $N_i$  receives  $(GID_j, GT_j)$  and stores them along with  $(ID_i, che_i)$  securely.

## V. LITEGAP: LIGHTWEIGHT GROUP AUTHENTICATION SCHEME

We propose a lightweight group authentication protocol, also called *liteGAP*, for IoD systems. In general, *liteGAP* is designed based upon lightweight operations such as bitwise XOR, hashing, and PUF operations. The basic idea of *liteGAP* is that the system is first initialized through ZSPs choosing and publishing a set of system parameters and functions, and drones selecting their real identities and PUF challenges. After system initialization, each drone can register with the ZSP by exchanging group authentication information and identity information. Finally, the ZSP will authenticate a group of drones and establish secure session keys with all drones simultaneously. Specifically, *liteGAP* is comprised of three stages to achieve the authenticated key establishment between a group of drones and the ZSP concurrently: (i) setup stage; (ii) registration stage; as well as (iii) group authentication and key establishment stage. In this paper, we choose drone  $N_i$  as a representative example to explain the operations in *liteGAP*. We also assume that a total of  $p$  drones, including drone  $N_i$  ( $i \leq p$ ), are deployed for the task/mission  $T_j$ . The mathematical symbols used in *liteGAP* and their meaning are provided in Table I.

### A. Setup Phase

In the setup phase, ZSP  $Z_s$  chooses system parameters and secure function, and drone  $N_i$  chooses its identity-related information. When the setup phase is over,  $Z_s$  will have a private key, while  $N_i$  will obtain its real identity and PUF challenge. The detailed steps are as follows.

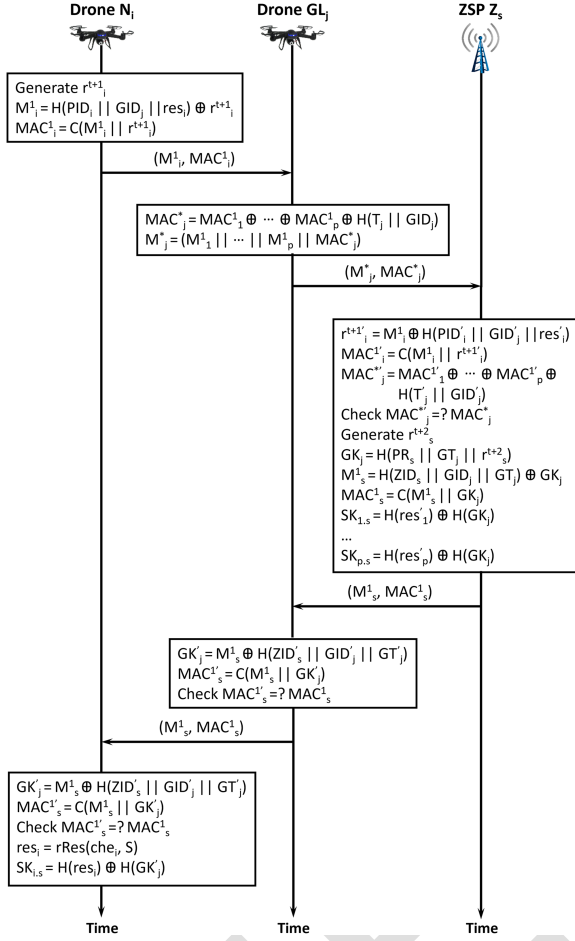


Fig. 3. Group authentication and key establishment phase.

### 445 C. Group Authentication and Key Establishment Phase

446 During the process of group authentication and key estab-  
 447 lishment, ZSP  $Z_s$  authenticates a pack of drones and reaches  
 448 an agreement on the secret session keys with all drones in the  
 449 group simultaneously. Fig. 3 presents the group authentication  
 450 and key establishment process of *liteGAP*, and its major steps  
 451 are explained below.

- 452 1) A group leader  $GL_j$  is selected based on fuzzy logic  
 453 algorithm which takes input as drones' residual energy  
 454 and the distances between drones and ZSP  $Z_s$  [26].
- 455 2)  $N_i$  generates a nonce  $r_i^{t+1}$  and calculates  $M_i^1 = H(PID_i$   
 456  $|| GID_j || res_i) \oplus r_i^{t+1}$ .  $N_i$  also calculates a message  
 457 authentication code (MAC)  $MAC_i^1 = C(M_i^1 || r_i^{t+1})$ .  
 458 Finally,  $N_i$  sends its authentication request  $(M_i^1, MAC_i^1)$   
 459 to  $GL_j$ .
- 460 3) When  $GL_j$  receives all authentication requests from the  
 461 group, it calculates an aggregate message authentication  
 462 code [27]  $MAC_j^* = MAC_1^1 \oplus MAC_2^1 \oplus \dots \oplus MAC_p^1$   
 463  $\oplus H(T_j || GID_j)$ . Here,  $p$  is the total number of drones  
 464 in the group.
- 465 4)  $GL_j$  generates an aggregate authentication request  $M_j^* =$   
 466  $(M_1^1 || M_2^1 || \dots || M_p^1 || MAC_j^*)$ , and sends  $(M_j^*, MAC_j^*)$   
 467 to  $Z_s$ .

- 5) After  $Z_s$  receives  $(M_j^*, MAC_j^*)$  from  $GL_j$ , it retrieves  
 468 drones' identity-related information and group authen-  
 469 tication related information from the database. Then, it  
 470 restores the nonce and computes the MAC for the authen-  
 471 tication request from each drone as the following. 472

$$r_i^{t+1} = M_i^1 \oplus H(PID_i || GID_j || res_i)$$

$$MAC_i^1 = C(M_i^1 || r_i^{t+1})$$

Here,  $Z_s$  can easily relate  $M_i^1$  to the corresponding PUF  
 473 response  $res_i$ . This is because  $Z_s$  obtains  $N_i$  real identity,  
 474 pseudonym, PUF challenge, and group authentication  
 475 information and stores them in the database during the  
 476 registration phase. 477

- 6)  $Z_s$  computes  $MAC_j^{*'} = MAC_1^1 \oplus MAC_2^1 \oplus \dots \oplus$   
 478  $MAC_p^1 \oplus H(T_j || GID_j)$ , and checks  $MAC_j^{*'} \stackrel{?}{=} MAC_j^*$ .  
 479 If they are equal,  $Z_s$  proceeds with the following steps.  
 480 Otherwise, the group authentication request is rejected. 481
- 7) Once the verification succeeds,  $Z_s$  generates a nonce  $r_s^{t+2}$   
 482 and calculates the group key  $GK_j = H(PR_s || GT_j ||$   
 483  $r_s^{t+2})$ . It also generates  $M_s^1$  and  $MAC_s^1$  and sends  $(M_s^1,$   
 484  $MAC_s^1)$  to  $GL_j$ . 485

$$M_s^1 = H(ZID_s || GID_j || GT_j) \oplus GK_j.$$

$$MAC_s^1 = C(M_s^1 || GK_j)$$

Then,  $Z_s$  establishes secure session keys for all drones in  
 486 the group as the following. 487

$$SK_{1,s} = H(res_1) \oplus H(GK_j)$$

$$SK_{2,s} = H(res_2) \oplus H(GK_j)$$

...

$$SK_{p,s} = H(res_p) \oplus H(GK_j)$$

Here, since  $Z_s$  will generate a different nonce each  
 488 time, the calculated group key will also be different. As  
 489 a result,  $Z_s$  is able to establish different secure session  
 490 keys with all drones during the group authentication and  
 491 key establishment stage. In other words, the secure session  
 492 keys will be frequently updated in our approach *liteGAP*. 493

- 8) On receiving  $(M_s^1, MAC_s^1)$  from  $Z_s$ ,  $GL_j$  retrieves the  
 494 group authentication related information and calculates  
 495 the following. 496

$$GK_j' = M_s^1 \oplus H(ZID_s || GID_j || GT_j')$$

$$MAC_s^1 = C(M_s^1 || GK_j')$$

After that,  $GL_j$  checks the validation of  $MAC_s^1 =$   
 497  $MAC_s^1$ . If they are equal,  $GL_j$  broadcasts  $(M_s^1, MAC_s^1)$   
 498 to all drones in the group. Otherwise, it discards the  
 499 message. 500

- 9) After receiving  $(M_s^1, MAC_s^1)$  from  $GL_j$ ,  $N_i$  first restores  
 501  $GK_j' = M_s^1 \oplus H(ZID_s || GID_j || GT_j')$ , and then verifies  
 502 whether  $MAC_s^1$  equals to  $MAC_s^1$  or not (similar to the  
 503 previous step). If the verification fails,  $N_i$  discards the  
 504 message. If the verification succeeds, it computes its own  
 505

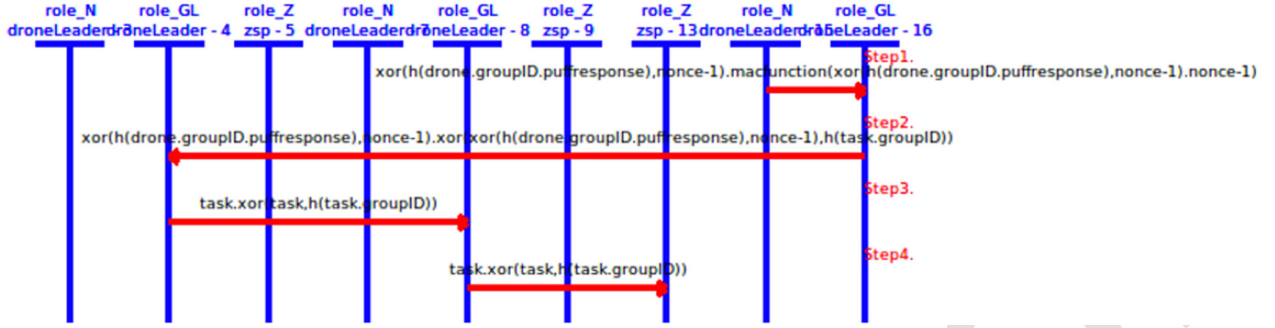


Fig. 4. Communication sequence diagram of AVISPA security verification.

506 secure session key as follows.

$$res_i = rRes(ch_{e_i}, S)$$

$$SK_{i,s} = H(res_i) \oplus H(GK_j')$$

507 By this time, the group authentication between all drones  
 508 in the group and ZSP  $Z_s$  is executed completely, and  
 509 secure session keys have been successfully established for  
 510 all drones to securely communicate with ZSP  $Z_s$ .

## 511 VI. LITEGAP'S RESILIENCE AND SECURITY ANALYSIS

### 512 A. Security Verification

513 Security protocols might have weaknesses which can be  
 514 exploited by the adversary to conduct serious attacks without  
 515 compromising cryptography, such as masquerading attacks or  
 516 replay attacks. Thus, we choose AVISPA [28], a tool for the  
 517 automatic verification of security protocols, to automatically  
 518 analyze and validate our approach *liteGAP*, and demonstrate  
 519 that *liteGAP* is able to work securely even under worst-case  
 520 adversarial environments. Typically, the to-be-validated security  
 521 protocol can be represented as a security problem in the HLP  
 522 (the programming language on AVISPA) [6], and then evaluated  
 523 against masquerading attacks, replay attacks, and other unknown  
 524 attacks on AVISPA. If the security protocol suffers from a  
 525 specific attack, AVISPA will display the vulnerable scenario as  
 526 a sequence diagram. Otherwise, the security protocol is marked  
 527 as "safe" by AVISPA.

528 AVISPA provides two evaluation components: On-the-fly  
 529 Model-Checker (OFMC) and Constraint-Logic-based Attack  
 530 Searcher (CL-AtSe). Specially, OFMC evaluates the security  
 531 protocol through falsification and bounded verification. CL-  
 532 AtSe is able to deal with algebraic properties of cryptographic  
 533 operators and associativity of message concatenation, as well  
 534 as detect type-flaw attacks. In Virtual Box [29], we first install  
 535 Ubuntu 10.04, and then set up and configure a fully-functional  
 536 SPAN+AVISPA [6] environment. The communication sequence  
 537 diagram of AVISPA security verification as well as the outputs  
 538 of OFMC and CL-AtSe are demonstrated in Figs. 4 and 5  
 539 respectively, showing that *liteGAP* is a safe security protocol and  
 540 secure against masquerading attacks, replay attacks, and other  
 541 unknown attacks. The HLP security verification programs are  
 542 available at the <https://github.com/congpu/liteGAP>.

<p>SUMMARY  <b>SAFE</b>                  DETAILS                  BOUNDED_NUMBER_OF_SESSIONS                  TYPED_MODEL                  PROTOCOL                  /home/span/testsuite/results/liteGAP.if                  GOAL                  as_specified                  BACKEND                  OFMC                  COMMENTS                  STATISTICS                  Analysed: 15 states                  Reachable: 15 states                  Translation: 0.01 seconds                  Computation: 0.00 seconds</p>	<p>SUMMARY  <b>SAFE</b>                  DETAILS                  BOUNDED_NUMBER_OF_SESSIONS                  PROTOCOL                  /home/span/testsuite/results/liteGAP.if                  GOAL                  as_specified                  BACKEND                  OFMC                  COMMENTS                  STATISTICS                  parseTime: 0.00s                  searchTime: 5.18s                  visitedNodes: 8593                  nodes depth: 3 plies</p>
(a)	(b)

Fig. 5. Security verification results using AVISPA's CL-AtSe and OFMC.

### 543 B. Formal Security Analysis

544 We provide a formal security analysis of *liteGAP*, which  
 545 focuses on sharing the secret information  $res_i$  between drone  
 546  $ID_i$  and ZSP  $Z_s$ . Here, the secret information  $res_i$  is used to  
 547 achieve the authentication and key establishment between drone  
 548  $ID_i$  and ZSP  $Z_s$ . The goal of formal security analysis is to prove  
 549 that  $res_i$  is a good shared secret between drone  $ID_i$  and ZSP  
 550  $Z_s$ . In other words, the secret information  $res_i$  should not be  
 551 accessed by any attacker. We adopt the inference rules proposed  
 552 by Mao and Boyd [30] to build the formal security analysis of  
 553 the secret information  $res_i$  in *liteGAP*. Moreover, according to  
 554 the operations in setup and registration phases, we can build the  
 555 following beliefs.

- 556 1)  $ID_i \models ID_i \stackrel{res_i}{\leftarrow} Z_s$  and  $Z_s \models Z_s \stackrel{res_i}{\leftarrow} ID_i$ : The initial  
 557 response  $res_i$  of drone  $ID_i$  is securely shared between  
 558 drone  $ID_i$  and ZSP  $Z_s$ .
- 559 2)  $ID_i \models Z_s \triangleleft \parallel ID_i$ : The real identify of drone  $ID_i$  is  
 560 known by ZSP  $Z_s$ .
- 561 3)  $ID_i \models ID_i \stackrel{PID_i}{\leftarrow} Z_s$  and  $Z_s \models Z_s \stackrel{PID_i}{\leftarrow} ID_i$ : ZSP  $Z_s$  saves  
 562 the pseudonym of drone  $ID_i$  in its database, while drone  
 563  $ID_i$  can compute its  $PID_i$  using its real identify and  
 564 response  $R_i^t$ .
- 565 4)  $ID_i \models ID_i \stackrel{GID_j}{\leftarrow} Z_s$  and  $Z_s \models Z_s \stackrel{GID_j}{\leftarrow} ID_i$ : The group  
 566 identity  $GID_j$  is securely shared between drone  $ID_i$  and  
 567 ZSP  $Z_s$ .

$$\begin{array}{c}
\frac{N_i \models \{N_i\} \triangleleft \ll rRes(\cdot) \wedge N_i \triangleleft \ll che_i \quad \wedge \quad N_i \models \{Z_s\} \triangleleft \ll res_i}{N_i \models \{N_i\} \triangleleft \ll res_i} \quad \wedge \quad \frac{Z_s \models \{N_i\} \triangleleft \ll rRes(\cdot) \wedge N_i \triangleleft \ll che_i \quad \wedge \quad Z_s \models \{Z_s\} \triangleleft \ll res_i}{Z_s \models \{N_i\} \triangleleft \ll res_i} \\
\frac{N_i \models \{N_i, Z_s\} \triangleleft \ll res_i}{N_i \models N_i \xleftrightarrow{res_i} Z_s} \quad \wedge \quad \frac{Z_s \models \{N_i, Z_s\} \triangleleft \ll res_i}{Z_s \models N_i \xleftrightarrow{res_i} Z_s}
\end{array}$$

Fig. 6. Proof that drone  $ID_i$  and ZSP  $Z_s$  believe that secret information  $res_i$  is only shared between themselves.

- 568 5)  $ID_i \models ID_i \xleftrightarrow{GT_j} Z_s$  and  $Z_s \models Z_s \xleftrightarrow{GT_j} ID_i$ : The group  
569 token  $GT_j$  is securely shared between drone  $ID_i$  and ZSP  
570  $Z_s$ .  
571 6)  $ID_i \models Z_s \triangleleft \ll r^{t+1}$  and  $Z_s \models ID_i \models \{Z_s\} \triangleleft \ll r^{t+1}$ : Drone  
572  $ID_i$  generates a new  $r^{t+1}$  each time.  
573 7)  $ID_i \models \#(res_i)$ : Drone  $ID_i$  generates a fresh  $res_i$  each  
574 time.

575 Fig. 6 demonstrates the formal security analysis of *liteGAP*  
576 with regards to sharing the secret information  $res_i$  be-  
577 tween drone  $ID_i$  and ZSP  $Z_s$ . The rationale behind prov-  
578 ing the security of secret information  $res_i$  is that  $res_i$   
579 is critical for the authentication as well as the establish-  
580 ment of session key. We first establish the statements,  
581  $ID_i \models ID_i \xleftrightarrow{res_i} Z_s$  and  $Z_s \models ID_i \xleftrightarrow{res_i} Z_s$ , and make them become  
582 the foundation of the logical proof. Second, the Good Key  
583 rule [30] is applied to the statements  $ID_i \models ID_i \xleftrightarrow{res_i} Z_s$  and  
584  $Z_s \models ID_i \xleftrightarrow{res_i} Z_s$ , respectively. The Good Key rule indicates  
585 that if  $ID_i$  believes that  $res_i$  is only available to  $ID_i$  and  $Z_s$   
586 ( $ID_i \models \{ID_i, Z_s\} \triangleleft \ll res_i$  or  $Z_s \models \{ID_i, Z_s\} \triangleleft \ll res_i$ ), and  $ID_i$   
587 knows that  $res_i$  is fresh ( $ID_i \models \#(res_i)$ ), then  $ID_i$  believes  
588 that  $res_i$  is a good shared secret information between  $ID_i$   
589 and  $Z_s$ . Third, we apply the Confidentiality rule [30] to prove  
590  $ID_i \models \{ID_i, Z_s\} \triangleleft \ll res_i$  and  $Z_s \models \{ID_i, Z_s\} \triangleleft \ll res_i$ . Before  
591 that, we need to show that  $res_i$  is a shared secret information  
592 between  $ID_i$  and  $Z_s$  ( $ID_i \models ID_i \xleftrightarrow{res_i} Z_s$  and  $Z_s \models Z_s \xleftrightarrow{res_i} ID_i$ ).  
593 Fortunately, the above statement is one of the initial beliefs,  
594 thus, the truth of the security claims  $ID_i \models ID_i \xleftrightarrow{res_i} Z_s$  and  
595  $Z_s \models ID_i \xleftrightarrow{res_i} Z_s$  are successfully proved. In summary, accord-  
596 ing to Fig. 6, it is strongly believed that the secret information  
597  $res_i$  is a good shared secret between drone  $ID_i$  and ZSP  $Z_s$ .

### 598 C. Informal Security Analysis

599 In the following, we will exhibit how *liteGAP* satisfies the  
600 pre-defined security requirements in Section IV.C. First of all,  
601 *liteGAP* can achieve group authentication between a group of  
602 drones and the ZSP. This is because the group leader drone first  
603 collects separate authentication request from a group of drones.  
604 Then, it generates and issues an aggregate authentication request  
605 to the ZSP. After that, the ZSP can verify the identity of each  
606 drone based on the separate authentication request. Moreover, a  
607 group of drones and the ZSP can reach an agreement on the secret  
608 session keys for future communications using *liteGAP*. After the  
609 group authentication succeeds, the ZSP will calculate the group  
610 key which will be utilized to produce the secret session key for  
611 each drone. Third, *liteGAP* can guarantee the confidentiality of  
612 messages exchanged in an open network because the messages

are encrypted using the established session key. Fourth, *liteGAP* 613  
614 can achieve integrity because a message authentication code  
615 (MAC) is generated for each exchanged message. Last but  
616 not least, *liteGAP* supports anonymous communication for IoD  
617 systems. The rationale is that each drone is using its pseudonym,  
618 rather than its real identity, in the exchanged messages. 618

*liteGAP* is also secure against many well-known security at- 619  
620 tacks. First, *liteGAP* can defend against physical capture attack.  
621 The attacker might capture drone  $N_i$  and retrieve its identity-  
622 related information stored in the memory, e.g.,  $ID_i$  and  $che_i$ ,  
623 through probing attack. However, the attacker is unable to obtain  
624 the critical cryptography-related information such as  $res_i$  from  
625 drone  $N_i$ . This is because the PUF of  $N_i$  will be destroyed and  
626 the original  $res_i$  cannot be regenerated whenever the attacker  
627 plans to retrieve  $res_i$  from  $N_i$ 's integrated circuit. Second,  
628 *liteGAP* is secure against replay attack. Since each message  
629 is piggybacked with timestamp  $ts$ , ZSP  $Z_s$  is able to verify  
630  $ts$ , and then detect and discard the replayed messages. Third,  
631 *liteGAP* is secure from drone impersonation attack. Suppose that  
632 an adversary wants to impersonate a legitimate drone  $N_i$  in order  
633 to establish authentication with ZSP  $Z_s$  to cause some financial  
634 and strategic damages. In order to send a valid authentication  
635 request to the group leader  $GL_j$ , e.g.,  $(M_i^1, MAC_i^1)$  on behalf  
636 of legitimate drone  $N_i$ , the adversary obtains the identifier of  
637 group leader  $GL_j$  and then generates a nonce  $r_i^{t+1}$ . However,  
638 without having the valid CRP  $(che_i, res_i)$  of legitimate drone  
639  $N_i$ , it is a difficult task for the adversary to generate the valid  
640  $M_i^1$  and  $MAC_i^1$  which can be correctly decoded by ZSP  $Z_s$ .  
641 As a result, the adversary cannot generate a valid authentication  
642 request on behalf of legitimate drone  $N_i$ . Thus, it is impractical  
643 for the adversary to impersonate drone  $N_i$ . Fourth, *liteGAP*  
644 generates message authentication code  $MAC$  to authenticate  
645 the corresponding message, thus, *liteGAP* can defend against  
646 message modification attack. Lastly, *liteGAP* is not vulnerable to  
647 man-in-the-middle attack. In *liteGAP*, ZSP  $Z_s$  first authenticates  
648 and establishes a secure session key with drone  $N_i$ . After that,  
649  $Z_s$  and  $N_i$  can safely communicate over an insecure channel,  
650 and the attacker is unable to replay and modify the transmitted  
651 messages. In summary, *liteGAP* can meet all required security  
652 requirements as outlined in Section IV.C., and the list of achieved  
653 security requirements is summarized in Table II. 653

## 654 VII. PERFORMANCE EVALUATION

### 655 A. Experimental Environment

656 We build an experimental framework on the MacBook Air  
657 laptop and conduct extensive experiments to evaluate the perfor-  
658 mance of *liteGAP*. An Eclipse simulation environment [31] is set 658



TABLE II  
ACHIEVED SECURITY REQUIREMENTS

Security Requirement	<i>liteGAP</i>
Group Authentication	Yes
Group Session Key Establishment	Yes
Confidentiality	Yes
Integrity	Yes
Anonymity	Yes
Replay Attack	Yes
Man-In-The-Middle Attack	Yes
Drone Capture Attack	Yes
Drone Impersonation Attack	Yes
Message Modification Attack	Yes
Known Session Key Attack	Yes
ZSP Spoofing Attack	Yes

TABLE III  
COMPARISON OF COMMUNICATION COST

Protocol	No. of Trans. Msg	Energy Consumption of Trans.
<i>liteGAP</i>	203	$2.29 \times 10^{-2}$
GASE	403	$4.54 \times 10^{-2}$
rampIoD	600	$6.76 \times 10^{-2}$

\*In this experiment, we assume that 200 drones form a group and want to authenticate and establish secure session keys with the ZSP simultaneously.

up on the MacBook Air laptop, where *liteGAP* and two benchmark schemes are implemented in Java programming language. The MacBook Air laptop runs macOS Ventura 13.3.1 operating system with Apple M2 chip (8-core CPU, 10-core GPU, and 16-core Neural Engine), and the size of unified memory and SSD hard drive are 8 GB and 512 GB, respectively.

### B. Benchmark Schemes and Performance Metrics

We choose two representative protocols, GASE [7] and rampIoD [8], as the benchmark schemes, and compare them with *liteGAP* for performance evaluation and analysis. rampIoD represents the typical authentication schemes which have been widely proposed in the IoD community, where a central authority authenticates the two entities (i.e., user and drone), and then helps them mutually authenticate each other and establish a session key. Since the current IoD community does not have similar group authentication technique, we have to select a group authentication protocol from a similar environment as another benchmark scheme. GASE is a group authentication protocol with key agreement feature which is proposed for edge computing environments. The basic idea of GASE and rampIoD are presented below:

- GASE: The objective of GASE is to validate and authenticate a mass of IoT devices without overburdening the central server in the cloud-edge-IoT environment. First, all registered IoT devices are divided into a number of groups, including one edge node and one group leader. Second, all members in the group are authenticated by the group leader using multi-secret sharing scheme. Third, the group leader sends the validated IoT devices' identifiers to the edge node. Lastly, the edge node combines all identifiers and transmits it to the central server for verification.
- rampIoD: rampIoD is designed to establish an authenticated communication between the user and the drone in the IoD environment. First, the IoD system is initialized through choosing and publishing the system parameters by the control room. Second, the drone and the user register themselves with the control room to obtain their secret credentials. Third, before the user and the drone can exchange any sensitive information securely, they are required to achieve the authentication with the control room first. Finally, with the assistance of the control room, the

user and the drone will establish a secure session key for future communication.

The performance of *liteGAP*, GASE, and rampIoD are measured in diverse performance metrics such as communication cost, run time, CPU time, as well as storage overhead. In the following, we provide the meaning of performance metric and explain how to measure and obtain the corresponding results.

- The communication cost is represented in terms of two sub-metrics, which are the number of transmitted messages and the energy consumption of message transmissions. Since the actual wireless communication between the IoD entities is not being simulated in the experiments, we just simply investigate *liteGAP* and two benchmark schemes, and count the number of transmitted messages. The energy consumption of message transmissions is the product of the number of transmitted messages and the energy consumption of sending and receiving a single message [32].
- The run time and the CPU time are very similar; both of them are measuring the total time elapsed from when the protocol begins execution to when the protocol finishes execution. However, the major difference between the run time and the CPU time is that the CPU time does not include the latency due to operating in low-power idle state as well as input/output operation delay.
- The storage overhead indicates how much memory space is required by the protocol.

We choose two experimental parameters, which are the number of drones in the network and the number of algorithm executions, to measure the results of performance metrics. The reason that we select the number of drones in the network as one of the experimental parameters is because this paper focuses on the group authentication protocol. By varying the number of drones in the network, we can easily observe the performance difference between our approach *liteGAP* and benchmark scheme GASE and rampIoD, and how much performance improvement our approach *liteGAP* can make. We also obtain the experimental results by changing the number of algorithm executions, which will help us observe the performance of all three schemes from a long-term running point of view.

### C. Performance Results and Analysis

First, the communication cost is presented in Table III, where the number of transmitted messages and the energy consumption of message transmissions are obtained for *liteGAP*, GASE, and rampIoD. In this experiment, we assume that 200 drones form a group and want to authenticate and establish secure session keys with the ZSP simultaneously. According to the communication

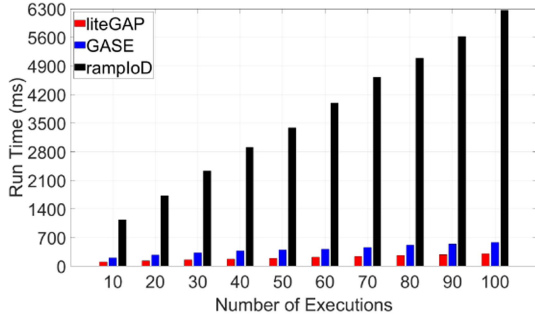


Fig. 7. Run time against the number of executions.

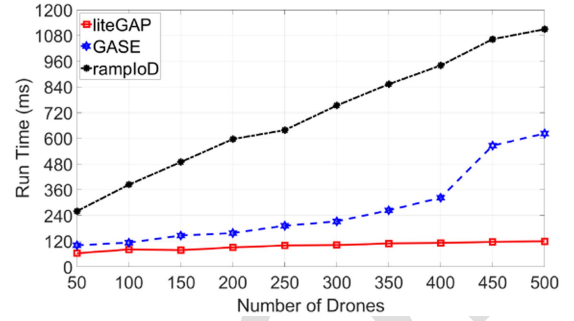


Fig. 8. Run time against the number of drones.

746 sequence diagram of rampIoD, a total of 600 messages are  
 747 required to be transmitted when a group of 200 drones are  
 748 considered. In fact, each drone is required to exchange three  
 749 (3) messages with the ZSP to successfully complete the process  
 750 of authentication and key agreement in rampIoD. In GASE, a  
 751 total of 403 messages are needed when a group of 200 drones  
 752 exist in the network. First, each drone sends a message to the  
 753 group leader drone for revealing its secret share, and then the  
 754 group leader drone broadcasts one confirmation message to all  
 755 drones. After that, each drone sends a message with the MAC  
 756 to the group leader drone. Finally, the group leader drone transmits  
 757 two messages to the authentication server for authenticating the  
 758 group. In summary, a total of 403 messages are transmitted  
 759 during the entire process. However, our approach *liteGAP* only  
 760 needs 203 messages exchanged between a group of 200 drones  
 761 and the ZSP. To be specific, the group leader drone first receives  
 762 an independent authentication request message from each drone  
 763 in the group. After that, two additional messages (e.g., aggregate  
 764 authentication request and authentication response messages)  
 765 will be exchanged between the group leader drone and the ZSP.  
 766 Finally, the authentication response message is broadcasted to  
 767 all other drones in the group by the group leader drone. To  
 768 sum up, 203 message transmissions are observed by *liteGAP*. In  
 769 addition, the energy consumption of message transmissions for  
 770 *liteGAP*, GASE, and rampIoD are  $2.29 \times 10^{-2}$ ,  $4.54 \times 10^{-2}$ , and  
 771  $6.76 \times 10^{-2}$ , respectively. Since our approach *liteGAP* requires  
 772 a less number of messages to be exchanged in the network, less  
 773 energy is consumed for wireless communication by *liteGAP*.

774 Second, the run time is measured by changing the number of  
 775 protocol executions, and the results are presented in Fig. 7. As  
 776 shown in Fig. 7, the run time of *liteGAP*, GASE, and rampIoD  
 777 become greater as the number of executions is increased from 10  
 778 times to 100 times. Since the protocols are executed repeatedly, a  
 779 longer run time will be required to run the protocols more times.  
 780 As a result, the overall run time of three schemes will obviously  
 781 experience an increment as the number of executions increases.  
 782 For rampIoD, it is always the most time-consuming protocol  
 783 when the number of executions is varied from 10 to 100 times.  
 784 This is because rampIoD is implemented based on heavy-weight  
 785 techniques such as authenticated encryption with associative  
 786 data and elliptic curve cryptography. It is widely known that  
 787 elliptic curve point multiplication is an expensive operation. As  
 788 a result, a longer time can be expected certainly when rampIoD

789 is executed. And when we change the number of executions, the  
 790 run time of rampIoD increases significantly. GASE is a group  
 791 authentication protocol designed for edge computing environ-  
 792 ments, where secret sharing scheme and aggregated message  
 793 authentication code are adopted to achieve the group authen-  
 794 tication. Compared to the techniques used in rampIoD, secret  
 795 sharing scheme and aggregated message authentication code  
 796 are regarded as light-weight operations, and they will take less  
 797 time to execute. Thus, GASE finishes the authentication process  
 798 more quickly, and a smaller run time is observed by GASE  
 799 when the number of executions is increased. Our approach  
 800 *liteGAP* shows the lowest run time compared to rampIoD and  
 801 GASE with a varying number of executions. Instead of executing  
 802 the same authentication scheme for each drone in the group,  
 803 *liteGAP* is able to realize the group authentication between a  
 804 drone swarm and the ZSP. Thus, the lowest execution time is  
 805 observed by *liteGAP*. Note that rampIoD has to execute the entire  
 806 authentication scheme for each drone in the group so that they  
 807 can achieve the group authentication. Even through GASE is  
 808 a group authentication protocol, however, it is not designed for  
 809 IoD systems and secret sharing scheme is more time-consuming  
 810 than the techniques used in *liteGAP*.

811 Third, we measure the run time of *liteGAP*, GASE, and ramp-  
 812 IoD by changing the number of drones in the network in Fig. 8.  
 813 Overall, the increasing number of drones in the network will  
 814 make the run time of all three schemes increase. The rationale  
 815 is that certain operations will be executed more times when  
 816 the number of drones is increased. Finally, a longer run time  
 817 is observed for all three schemes. *liteGAP* and GASE show a  
 818 lower run time than rampIoD because rampIoD is a one-to-one  
 819 authentication protocol, not a group authentication protocol.  
 820 When the network has more drones, it is obvious that rampIoD  
 821 will take more time to authenticate them because each drone  
 822 will need a separate authentication. The run time of *liteGAP* is  
 823 lower than that of GASE because the run time of secret sharing  
 824 scheme in GASE significantly increases when the number of  
 825 drones increases in the network.

826 Fourth, the CPU time of *liteGAP*, GASE, and rampIoD are  
 827 measured against the number of executions and the number of  
 828 drones in Fig. 9 and Fig. 10, respectively. Unlike the run time,  
 829 the CPU time does not include the latency due to operating in  
 830 low-power idle state as well as input/output operation delay. As  
 831 shown in Fig. 9, an increasing number of executions results in

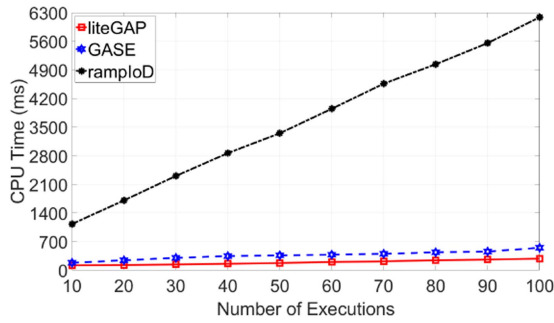


Fig. 9. CPU time against the number of executions.

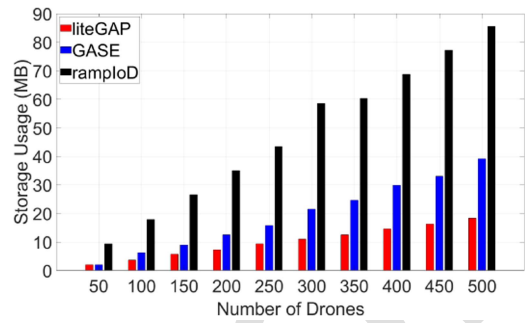


Fig. 11. Storage usage against the number of drones.

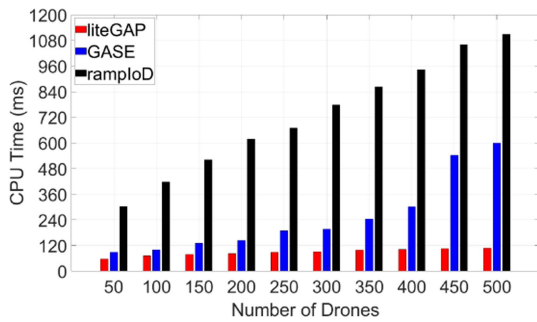


Fig. 10. CPU time against the number of drones.

TABLE IV  
COMPARISON OF AVERAGE STORAGE USAGE

Protocol	No. of Drones	Avg. Storage Usage
<i>liteGAP</i>	200	7.34 MB
GASE	200	12.50 MB
rampIoD	200	35.00 MB

lower than that of GASE and rampIoD. When the IoD system comprises 200 drones, the storage space required by *liteGAP* is approximately 7.34 MB. However, for GASE and rampIoD, 12.5 MB and 35 MB storage space are consumed, respectively. The reason behind this interesting result is that our approach *liteGAP* adopts lightweight operations which execute faster and use less storage space. GASE and rampIoD use more complex operations such as secret sharing scheme and authenticated encryption with associative data scheme, respectively. Thus, more storage space is consumed by them.

### VIII. CONCLUDING REMARKS AND FUTURE WORK

In this paper, we focused on the issue of information privacy and security in the IoD environment, and then designed *liteGAP*, a lightweight group authentication protocol, for IoD systems. With *liteGAP*, a drone swarm and the ZSP can realize the authenticated key establishment concurrently. We first implemented *liteGAP* in HPLSL and performed a security verification on AVISPA, and *liteGAP* is believed to be secure and there is no security weaknesses. Moreover, we conducted a formal and informal security assessment on *liteGAP*, showing that *liteGAP* meets all the pre-defined security requirements. Finally, we built an experimental simulation framework, implemented *liteGAP* and its counterparts in Java, and then evaluated and analyzed their performance. The experimental results showed that *liteGAP* can provide better performance than the state-of-the-art schemes.

Although *liteGAP* outperforms existing schemes, we still see potential for further improvements. To be specific, *liteGAP* does not support cross-domain group authentication that the drones authenticate with the ZSPs located in different physical domains. Nonetheless, how to realize the process of authentication and key agreement between a group of drones and different ZSPs in the IoD environment is a non-trivial problem. Recently, some researchers adopt blockchain technique to resolve the issue of

an increment in CPU time for all three schemes. However, our scheme *liteGAP* still demonstrates the lowest CPU time because of the adoption of lightweight operations such as bitwise XOR, PUF, and hash function. In addition, the group authentication between multiple drones and the ZSP can be achieved by our scheme *liteGAP*, thus, the number of authentication operations is reduced and a lower CPU time is obtained. A lower CPU time is also obtained by GASE compared to rampIoD, because GASE is designed for group authentication with light-weight techniques (i.e., secret sharing scheme and aggregated message authentication code). The highest CPU time belongs to rampIoD because it adopts resource-hungry techniques such as authenticated encryption with associative data and elliptic curve cryptography. Fig. 10 also shows that our approach *liteGAP* provides the lowest CPU time as the number of drones is increased from 50 to 500.

Fifth, we obtain the storage usage of *liteGAP*, GASE, and rampIoD by changing the number of drones, and present the results in Fig. 11. rampIoD requires the largest amount of memory storage to run. This is because the authenticated encryption with associative data and elliptic curve cryptography are more complex than the techniques being used in both *liteGAP* and GASE. As a result, more space would be needed for instructions, environmental stack, as well as data by rampIoD. Compared to secret sharing scheme and aggregated message authentication code, bitwise XOR, PUF, and hash function do not have high storage demand. Thus, a lower storage usage is obtained by our approach *liteGAP*.

Finally, in Table IV we measure and present the results of average storage usage for *liteGAP*, GASE, and rampIoD. Overall, the average storage usage of our approach *liteGAP* is much

cross-domain authentication. Unfortunately, these blockchain-based security protocols require the frequent update of cryptographic information stored in the blockchain, which incurs a very high communication and computation overhead. As a future work, we plan to look into this potential problem, and propose a lightweight cross-domain group authentication protocol for the IoD systems.

## REFERENCES

- [1] Commercial Drone Market. Accessed: Apr. 25, 2022. [Online]. Available: <https://www.grandviewresearch.com/>
- [2] P. Boccadoro, D. Striccoli, and L. Grieco, "An extensive survey on the internet of drones," *Ad Hoc Netw.*, vol. 122, 2021, Art. no. 102600.
- [3] S. Hussain, S. Chaudhry, O. Alomari, M. Alsharif, M. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for Internet of Drones," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021.
- [4] Y. Wu, H. Dai, H. Wang, and K. Choo, "Blockchain-based privacy preservation for 5G-enabled drone communications," *IEEE Netw.*, vol. 35, no. 1, pp. 50–56, Jan./Feb. 2021.
- [5] X. Yan and M. Ma, "A privacy-preserving handover authentication protocol for a group of MTC devices in 5G networks," *Comput. Secur.*, vol. 116, 2022, Art. no. 102601.
- [6] L. SPAN.: Jun. 29, 2023. [Online]. Available: <http://people.irisa.fr/Thomas.Genet/span/>
- [7] M. Nakkar, R. AlTawy, and A. Youssef, "GASE: A lightweight group authentication scheme with key agreement for edge computing applications," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 840–854, Jan. 2023.
- [8] M. Tanveer, A. Khan, N. Kumar, and M. Hassan, "RAMP-IoD: A robust authenticated key management protocol for the internet of drones," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1339–1353, Jan. 2022.
- [9] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.
- [10] G. Li and C. Lai, "Platoon handover authentication in 5G-V2X: : IEEE CNS 20 Poster," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2020, pp. 1–2.
- [11] M. Abdel-Malek, K. Akkaya, A. Bhuyan, and A. Ibrahim, "A proxy signature-based drone authentication in 5G D2D networks," in *Proc. IEEE 93rd Veh. Technol. Conf.*, 2021, pp. 1–7.
- [12] A. Yazdinejadna, R. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Netw.*, vol. 120, 2021, Art. no. 102574.
- [13] S. Zhang and J. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4557–4565, May 2020.
- [14] Z. Shang, M. Ma, and X. Li, "A secure group-oriented device-to-device authentication protocol for 5G wireless networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7021–7032, Nov. 2020.
- [15] A. Lizardo, R. Barbosa, S. Neves, J. Correia, and F. Araujo, "End-to-end secure group communication for the Internet of Things," *J. Inf. Secur. Appl.*, vol. 58, 2021, Art. no. 102772.
- [16] A. Yang et al., "Privacy-preserving group authentication for RFID tags using bit-collision patterns," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11607–11620, Jul. 2021.
- [17] A. Miglani and N. Kumar, "Blockchain-based co-operative caching for secure content delivery in CCN-enabled V2G networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5274–5289, Apr. 2023.
- [18] A. Miglani, N. Kumar, A. Kishore, and N. Mohammad, "UAV-enabled edge computing and blockchain based secure charging station selection for energy trading in V2G environment," in *Proc. ACM DroneCom, 2022*, pp. 103–108.
- [19] M. Mispan and B. Halak, "Physical unclonable function: A hardware fingerprinting solution," in *Authentication of Embedded Devices*. Berlin, Germany: Springer, 2021, pp. 29–51.
- [20] J. Wallrabenstein, "Practical and secure IoT device authentication using physical unclonable functions," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud*, 2016, pp. 99–106.
- [21] F. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, the Netherlands: Elsevier, 1977.
- [22] Q. Do, B. Martini, and K. Choo, "The role of the adversary model in applied security research," *Comput. Secur.*, vol. 81, pp. 156–181, 2019.
- [23] W. Chen, Y. Dong, and Z. Duan, "Manipulating drone position control," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2019, pp. 1–9.
- [24] W. Stallings, *Cryptography and Network Security - Principles and Practices*, 8th Ed. London, U.K.: Pearson, 2020.
- [25] D. MRaihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-based one-time password algorithm," Internet Eng. Task Force, Fremont, CA, USA, RFC 6238, May 2011.
- [26] G. Jayaraman and V. Dhulipala, "FEECS: Fuzzy-based energy-efficient cluster head selection algorithm for lifetime enhancement of wireless sensor networks," *Arabian J. Sci. Eng.*, vol. 47, pp. 1631–1641, 2022.
- [27] J. Katz and A. Lindell, "Aggregate message authentication codes," in *Proc. Topics Cryptol.*, 2008, pp. 155–169.
- [28] "Automated validation of internet security protocols and applications." Accessed: Jun. 29, 2023. [Online]. Available: [https://www.ercim.eu/publication/Ercim\\_News/enw64/armando.html](https://www.ercim.eu/publication/Ercim_News/enw64/armando.html)
- [29] Last VirtualBox. Accessed: Jun. 29, 2023. [Online]. Available: <https://www.virtualbox.org/>
- [30] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *Proc. IEEE Comput. Secur. Found. Workshop*, 1993, pp. 147–158.
- [31] L. Eclipse. Accessed: Jun. 29, 2023. [Online]. Available: <https://www.eclipse.org/downloads/>
- [32] C. Pu and S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: Design, analysis, and evaluation," *IEEE Syst. J.*, vol. 12, no. 1, pp. 834–842, Mar. 2018.