Computer Networks 225 (2023) 109664

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era

B.D. Deebak, Seong Oun Hwang *

Department of Computer Engineering, Gachon University, Seongnam, South Korea

ARTICLE INFO

Keywords:
Unmanned aerial vehicle
B5G/6G
Aerial ad hoc network
Multi-factor authentication
Artificial intelligence
Security

ABSTRACT

In the diverse range of surveillance applications, large-scale deployment of next-generation communication technologies and the fast-growing development of unmanned aerial vehicles (UAVs) are envisioned as key innovations in the adoption of beyond-fifth generation (B5G) and 6G communication. Due to its self-reliance and versatility, a complex communication network can be formulated strategically to improve the application features of drone technology, including search-and-rescue, mission-critical services, and military surveillance. In recent times, technological advancements in hardware and software infrastructure have gained momentum toward seamless information interaction in aerial communication. Unfortunately, the recurrent process of user authentication causes severe communication instability in an unmanned aerial ad hoc network (UAANET) leading to some serious cyber threats, such as buffer overflow, denial of service, and spoofing. Therefore, building secure and reliable authentication is inevitable in order to protect drone-aided healthcare service environments. To protect aerial zones and improve security efficiency, this paper designs robust lightweight secure multi-factor authentication (RL-SMFA). The proposed RL-SMFA utilizes an AI-enabled, secure analytics phase to verify the genuineness of drone swarms for the ground control station. While protecting communication with drone vehicles, we also observe that power consumption by drones is reduced to a large extent. Using formal verification under a random oracle model, we show that the proposed RL-SMFA can functionally resist system vulnerabilities and constructively decrease the computation and communication costs of the UAANET. Lastly, the simulation study using ns3 shows that the proposed RL-SMFA achieves better performance efficiencies in terms of throughput rate, packet delivery ratio, and end-to-end delay than other state-of-the-art approaches to discovering a proper link establishment.

1. Introduction

Unmanned aerial vehicles (UAVs) have been widely utilized for various mission-critical applications such as surveillance, aerial photography, asset inspection, search-and-rescue, and disaster response. A specific network controller coordinates aerial vehicles that monitor the airspace in order to offer a better navigation service [1]. UAVs offer critical services in several application domains ranging from military machines to civilian systems. Most of those domains are cost-effective to ensure survival and safety that highly rely on sensory technologies and communication standards. However, the state of the vehicles cannot be observed during flight. To determine a vehicle's condition in a real-time scenario, it is necessary to collect sensory information, possibly establishing a smart control system to recognize a dangerous situation. It is necessary to examine the conditions of the aerial vehicles that manage operational resources to optimize the resulting analyses. Each aerial vehicle operates various devices, such as sensors, a control center, a speed controller, the drone motor, and a memory unit, which typically demand more energy to control the navigation systems.

The network controller can define a fly zone to obtain information required by the communications system. It has a dedicated control room to inspect aerial information remotely, which has inbuilt sensors to sense physical phenomena via wireless technologies such as radio navigation, airbands, cellular data services, and low-power wide-area networks. Moreover, a server system connects the control room to inspect drone boxes in the aerial vehicles. Each vehicle authorizes users and a server system to establish secure communications. It can adhere to security properties (namely, perfect secrecy, device anonymity, and untraceability) to increase system efficiency. Fig. 1 shows a generic architecture for UAVs that realizes the potential benefits from communications

* Corresponding author.
E-mail address: sohwang@gachon.ac.kr (S.O. Hwang).

https://doi.org/10.1016/j.comnet.2023.109664
Received 24 October 2022; Received in revised form 30 January 2023; Accepted 26 February 2023
Available online 1 March 2023

systems [2]. There are different real-time entities, such as aerial vehicles, the control room, servers, and users, that access data through a specific fly zone. The architecture considers the server a trusted entity; thus, the aerial vehicles might be compromised under various attacks via wireless channels, such as forgery or impersonation, or by a privileged insider.

Healthcare industries, including diagnostics, preventive medicine, therapeutic treatments, manufacturers, and insurance firms, apply wireless technologies to enable a mobility scenario for information systems. These technologies might focus on the wireless medical system to examine security features that improve the service quality of healthcare units. Modern technology integrates advanced wireless technologies to reduce healthcare costs and develop new drugs and medical treatments. Healthcare systems implant body area networks (BANs) to analyze patient data, such as posture, blood oxygen level, and respiratory rate [3]. They utilize wireless technologies to integrate numerous implantable medical devices that apply a suitable prediction model to inspect select criteria that indicate conditions such as heart disease, diabetes, and chronic pain. Due to data ubiquity, medical providers prefer wearable devices to analyze chronic conditions. Of late, the Internet of Everything (IoE) has integrated the essential elements of healthcare systems for the development of chronic disease management.

Development of the information society offers pervasive connectivity and network services to design unmanned aerial vehicles using artificial intelligence. This intelligent design has a high potential for autonomy in drone communications governing some significant roles in logistics and transportation. To meet the challenges in drone mobility and network complexity, technical requirements such as data security and device protection are carefully studied. These requirements transform the utility of multi-sensory devices in order to carry significant computation resources such as channel access and memory storage. To integrate application systems, the IoT provides a horizontal structure to different network domains. The information society represents various IoT architectures to meet business constraints, including pervasive connectivity and network services. IoT architectures, including sensor-actuator and gateway data acquisition, use this horizontal structure to integrate system components that connect applications and devices in order to interact with diverse network domains. In the medical field, smart healthcare systems interconnect various computing devices to transfer patient data without human interference, monitoring and controlling the activities of wearable or implantable devices [4].

A clinical diagnosis uses a distributed database to maintain decentralized information in electronic form. Each analysis transforms a conventional diagnosis into smart telematics to perform web-based security assessment and provide disease management systems. These interconnected technologies utilize network-enabled devices, including the Internet of Medical Things (IoMT), for data acquisition and processing to facilitate the use of healthcare information in decision and control systems. The IoMT applies a self-organizing network with wireless medical sensor networks (WMSNs) to monitor health conditions and to transport patient records to participating entities over a dedicated wireless channel. The self-organizing network uses a few predefined interfaces such as code optimization, parameter compliance, and node integration to regulate the processing capabilities of WMSNs via associated software components. Mobile/cellular networks can adjust the configuration of their operational parameters to manage network congestion and energy saving. To build a robust network with low computation cost, the integrated B5G core adopts a dedicated module with central management of authentication procedure.

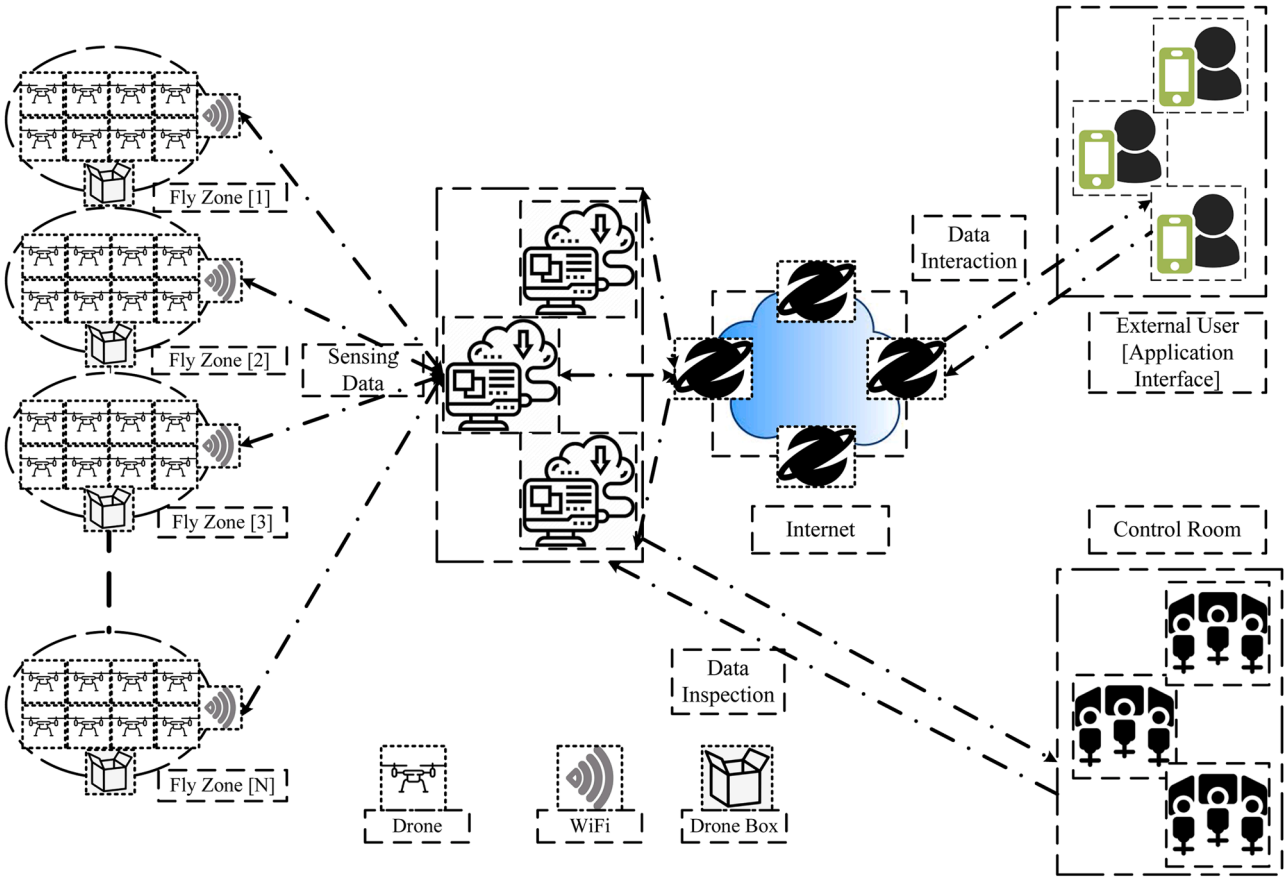

Fig. 1. A generic architecture for unmanned aerial vehicles.

1.1. Motivations behind the research

The appearance of lethal epidemics and pandemics highlights the significance of healthcare systems and the appropriate measurement strategies to generate genuine results. An airborne disease can trigger several biosensors monitoring blood pressure, cardiology signals, and pulse rate in order to diagnose medical conditions. The remote server explores the functional features of wearable sensing devices to enhance efficient data collection and analysis, which builds information modeling to monitor the occupational safety of the patient. To protect user privacy, various key agreement techniques have been introduced, such as authentication, shared secret keys, and key exchange [5]. Each technique guarantees the secure transmission of data containing sensitive information of a patient via highly reliable communications standards, e.g., IEEE 802.15.6. In practice, this standard can offer a few basic benefits, such as low power, fast data rates, and high quality of service, in deploying a BAN. However, to prevent potential threats, secure authentication and key agreement mechanisms are preferred.

For instance, medical surveillance systematically assesses the components that sense things like blood pressure, pulse oximetry, and body temperature to monitor the health of the patient remotely via dedicated cellular systems. The surveillance system discovers communication entities such as servers and medical practitioners for storing and analyzing medical data upon successful user authentication, and to recommend remote consultants and treatment follow-up. As a result, life-threatening emergencies such as cardiac arrest, breathing problems, and choking can be addressed in a timely manner to prevent the patient's condition from getting worse [6]. Because surveillance operates wirelessly in healthcare systems, an attacker might compromise the sensing units in order to launch intrusions like denial of service, identity replication, selective forwarding, and key disclosure [7]. To protect the surveillance systems including healthcare, the evolving infrastructure diverse its access types with communication service providers.

Hardware security module exposes different characteristics of B5G core network such as high bandwidth, data rate, and latency with edge computing systems to create a large-scale sensitive application. The application utilizes the capabilities of self-organizing networks to optimize the performance of mobile networks and enable operational intelligence to enhance the behavior of machine-to-machine (M2M) communication. Since M2M demands additional privacy preservation at the edge of the mobile networks, the privacy of data over LTE depends upon multi-access technologies to protect the coverage area of wireless Internet. Moreover, the communication technologies including B5G virtualize network functions to sense different type of healthcare services which demands a proper authentication to secure its customized networks leveraged by self-organizing networks. Therefore, a robust authentication technique is highly recommended to secure data transmissions for medical screening and surveillance that adopts deployment of the IoT surveillance [8,9].

1.2. Major contributions

Lately, the IoT and beyond-fifth-generation (B5G) and 6 G technologies have gained significant popularity due to the ever-changing demands of the network environment. The demand for appraisals enhances the properties of wireless networks in designing and building intelligent systems [10]. Such systems can utilize basic elements of the IoT to evaluate risk and impart device intelligence by using AI to improve the performance of next-generation networks [11]. The next-generation network utilizes physical and virtual devices to analyze a massive amount of sensitive data and provide a better decision-making process. In particular, medical surveillance includes various real-time objects to identify potential hazards and to conduct proper examinations, along with collecting medical histories [12]. To impart the learned intelligence, IoT environments employ web-based applications using different communications sources to interpret the defects of concern and emerging hazards in a surveillance zone. However, the IoT already addresses a few of the security challenges, such as weak authentication, data confidentiality, and privacy leakage [13]. Thus, this paper applies a complex cryptography mechanism to design robust lightweight secure multi-factor authentication (RL-SMFA). The main contributions are as follows.

1 Present robust lightweight secure multi-factor authentication using elliptic-curve cryptography (ECC) that utilizes an AI-enabled secure analytics phase to verify the authenticity of a drone via the trusted gateway.
2 Use an unmanned aerial ad hoc network (UAANET) to cover the standard requirements of the surveillance zone, including data confidentiality, sensor privacy, and security of the model.
3 Utilize a lightweight function and shared authentication to provide a strategic solution to authenticate the computing devices in drone surveillance.
4 Apply formal verification under a real-or-random model to examine the significant benefits of the proposed RL-SMFA, such as session key agreement and proper mutual authentication.
5 Evaluate the key agreement phase of the proposed RL-SMFA with other state-of-the-art approaches to assess the rate of energy consumption.

The remaining sections of this work are as follows. Section 2 discusses drone network architectures and related work to address communication patterns and security challenges in integrating the IoT with drone surveillance. Section 3 demonstrates a typical architecture for military zone surveillance, and discusses the relevant security goals, mathematical primitives, and threat models to analyze the standard constraints on healthcare authorities in the medical field. Section 4 presents the proposed RL-SMFA to address the challenges of medical surveillance systems. Section 5 discusses both formal and informal analysis to verify the security efficiency of the surveillance system. Section 6 presents a performance analysis of the RL-SMFA and other existing schemes that signify signaling, communication, computation, bandwidth, and energy utilization efficiency rates. Section 7 summarizes the cost efficiencies and simulation analysis of the proposed RL-SMFA and other existing schemes. Section 8 concludes the research.

2. Research background

The world has shown significant improvement in the ability to gain access to drone communications, which continuously creates global demand for various aerial applications in areas such as payload carriers, agriculture, bird control, and remote inspections. The establishment of drone networks has become more pervasive for industrial automation, which can open up new opportunities to enhance the operational efficiencies of any decision-making process. Such networks can provide a birds-eye view of navigation that applies network intelligence to identify malicious users, including cyber criminals. These networks have an onboard system that operates autonomously and that can efficiently engage or track targets in any hostile environment. Emerging applications such as fire monitoring, search-and-rescue operations, and racing drones demand aerial communication to accomplish key features like mobility and location awareness. As a result, functional parameters such as bandwidth, seamless communication, and uninterrupted services are tactfully adapted to manage any emergency-based ad hoc scenario. Aerial vehicles can be employed in either group-based or self-reliant mode to monitor any surveillance area, including battlefields and natural disasters.

It is worth noting that multiple aerial vehicles or network drones can spread out to perform tasks such as aerial-to-aerial and aerial-to-ground-station communication. They can collect and deliver information on floods, watersheds, and wildfires to devise a safe operational plan. Most networking environments demand reliable security because they rely on

resource-constrained wireless devices. On the other hand, aerial vehicles or drone networks require robust hardware to prevent unauthorised activity, such as network intrusions. One assignment is to monitor hostile environments that may include cyberattacks such as man-in-the-middle, SQL injection, drive-by download, cross-site scripting, password interception, and eavesdropping. As a result, an intruder may gain access to infer the secret key of a device and access sensitive data. As intelligent drones evolve, they integrate smart sensors, such as thermal, chemical, time-of-flight, and light-pulse distance sensors, and even radar.

Intelligent drones are often controlled without human intervention, which expands the scope of a human surveillance system. In general, such systems occupy less airspace to evaluate and monitor physical observations. Most countries apply drone codes to regulate system parameters such as frequency band, cost, range, interference, and barriers. They may exploit drone vulnerabilities to classify violation codes, including security and privacy.

2.1. Drone networks: security and privacy concerns

Drones serve as cost-saving technology to minimize health risks, which can provide reliable inspection over a comprehensive range of movement. They can regulate a broad spectrum not only to control advanced drone technology but also to operate in a surveillance area with minimum resources. They have numerous ways to learn about safety features, workforces, operational activities, threat scenarios, and hazardous elements, offering location tracking, an expanded mobility range, secure inspections, and data precision. Most drone models render safety surveillance to detect natural catastrophes. These features may even be classified as aerial imaging to identify hazardous elements of any disaster area, such as oil and gas refineries. However, a drone network is still challenged when trying to address three major concerns: safety, security, and privacy. The national-level addresses breaches of security and privacy and can strictly limit accessibility without the proper authorization to any comprehensive analysis, including image capture, video recordings, and location tracking. The security and privacy concerns of the drone network differ from those of conventional wireless networks, such as wireless sensor networks and mobile ad hoc networks.

A public safety network can carry smaller payloads and can reduce power consumption, computations, communications, and storage to achieve a better performance ratio. It has been shown that a drone network covers a bigger area than wireless networks. As a result, the security and privacy challenge primarily correlate to resources and delay constraints of aerial communications. Moreover, an aerial vehicle should ensure some key properties, such as availability, integrity, non-repudiation, authentication, and confidentiality, to obtain connectivity of any channel access. A drone meets the following guidelines:

- ***Authorization*** offers some privileges to an assignee to control aerial vehicles.
- ***Authentication*** exploits multi-factor authentication such as strong passwords, usernames, and biometrics to secure data transmission.
- ***Accounting/Auditing*** tracks the owners' legitimacy to infer whether there is any criminal or malicious activity trying to confine administration control.

A drone network might try to conduct malicious activities such as physical and cyber attacks. It may threaten public safety or breach the private information of any individual residence. It is worth noting that various technical properties are continuously exploited to launch potential attacks such as the distributed denial-of-service. Critical operations include offensive reconnaissance to track and locate specific activities of the people. This may cause severe security and privacy issues for drone networks. On the other hand, aerial surveillance is essential to protecting domestic and commercial zones, which demands drone photography to analyze safety breaches. Drone networks connect with wireless devices to gain internal access via dedicated signaling protocols that measure the security vulnerabilities to protect service connectivity. Most of the security assumptions employ single-user authentication to protect communications. Regrettably, an intruder can interfere with key generations to tamper with privacy information since it does not have any proper encryption mechanism to strengthen the security level. Fig. 2 shows classifications of cyber threats in drone networks.

2.2. Related work

In the past, various authentication frameworks have been introduced to guarantee user privacy, access control, and information security. To achieve secure communications in cloud computing, Islam and Biwas [14] designed multi-factor authentication using an elliptic-curve cryptosystem. Sarvabhatla and Vorugunti [15] showed that the scheme of Islam and Biwas cannot prevent vulnerabilities such as impersonation, privileged insider, password guessing, etc., which weakens the security level of computing systems. Also, they improved the mutual authentication framework with security and flexibility to validate user legitimacy. But rigorous analysis proved that the scheme of Sarvabhatla and Vorugunti is inefficient for resource-constrained application systems since it has an expensive computation cost. Kalra and Sood [16] constructed a key agreement mechanism using ECC for cloud computing in the IoT. Kumari et al. [17] demonstrated the security weaknesses of Kalra and Sood's approach, and improved their mechanism to offer better security efficiencies. Chang et al. [18] devised a remote identity-based authentication mechanism using ECC to analyze the significance of session key agreement.

Mo et al. [19] pointed out that the mechanism of Chang et al. cannot resist the smartcard loss attack. Fan et al. [20] designed a cloud-based lightweight authentication mechanism to solve cloud platform problems such as security and reliability. Deebak et al. [21] showed that most of the existing schemes [22–24] cannot prevent password guessing, and thus, cannot preserve client anonymity and provide proper secure mutual authentication. Hassanalian and Abdelkefi [22] reviewed the classification of flying drones to discuss challenges including design and fabrication. In addition, they discussed the issues of various navigation and control techniques to highlight the limitations of drone networks, such as sensing, communication, and coordination. Gharibi et al. [23] designed a strategic model to understand the key aspects of a large-scale network. A typical network explores a novel architecture to examine air traffic control and network management. Hall et al. [24] analyzed the available opportunities of drone operations to identify classes and non-compliance in drone communications. Won et al. [25] designed a communication protocol to examine three different application scenarios to handle massive real-time objects as they transfer complex data to available smart computing devices [18].

Several authentication schemes [28–39,32] utilized elliptic-curve cryptography and XOR operators to strengthen the security level. As a result, they do not exploit a technique for key exchange to satisfy the requirements of secret session key agreements between real-time entities. The Rivest-Shamir-Adleman algorithm was applied with a basic strategy for key exchange that generates a digital signature to negotiate an authentication process between two or more computing devices [26]. The elliptic-curve cryptography technique exploited a key exchange mechanism not only to optimize operational costs but also to limit the processing capacity of any intelligent device [27]. Ayub et al. [28] utilized authentication factors such as biometrics, smartcards, and the password-based approach to automate the process of key verification. System parameters such as nonce, timestamps, and challenge-responses were considered significant contributions to optimizing the complexity of the mutual authentication model. Kiran et al. [29] proposed two-factor lightweight authentication for cloud-based IoT environments. Rao et al. [30] and Loffi et al. [31] designed multi-factor user

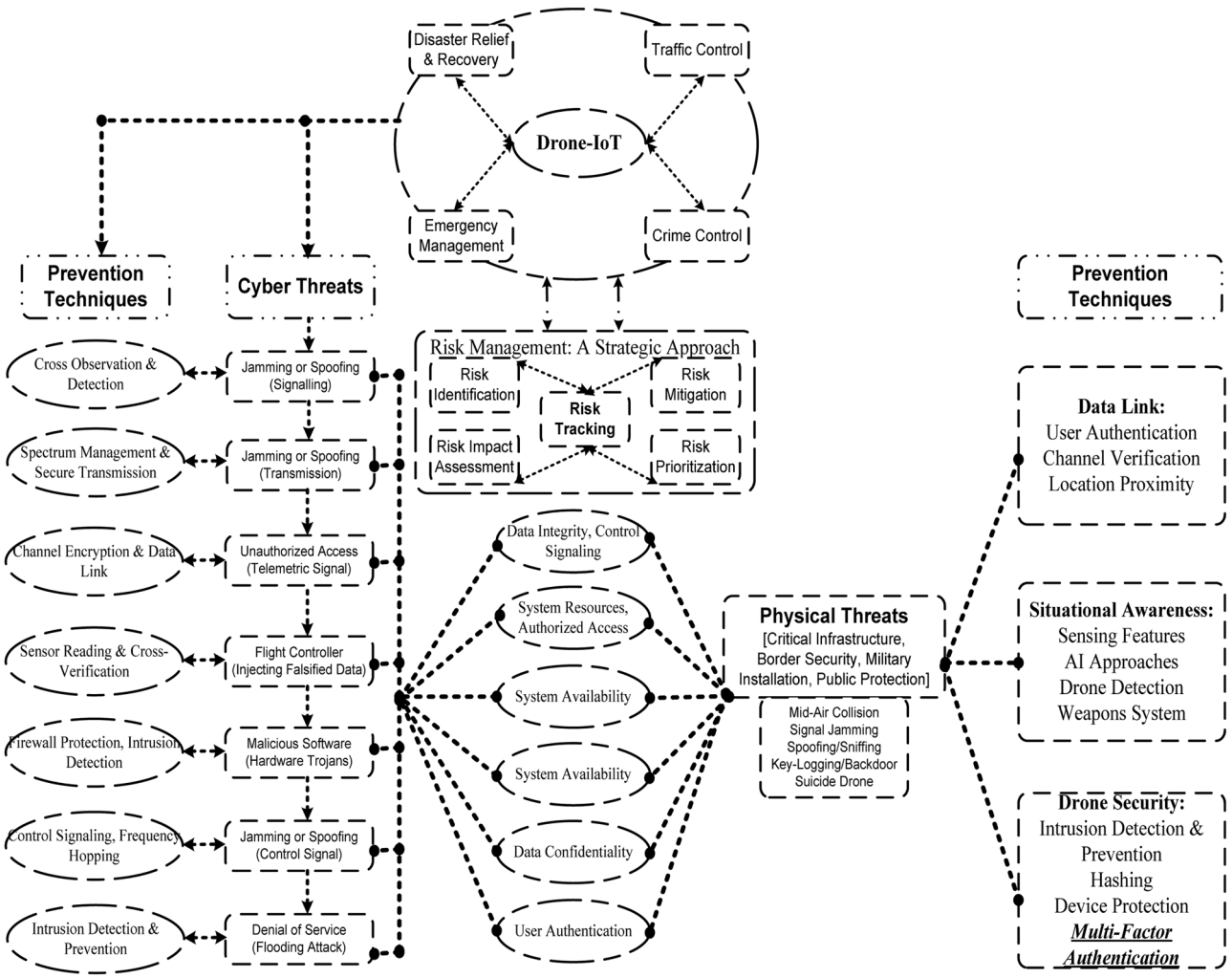

Fig. 2. Classification of cyber threats in drone networks.

authentication for fog computing. Their schemes deal with a challenge-response function to provide a reliable authentication model, using formal security proof to represent the complexity of the authentication protocols [32].

Zhang et al. [44] constructed an intelligent anonymous authentication and key agreement for vehicular ad hoc networks. This anonymous authentication uses 5 G/B5G networks to analyze the security efficiency of drone communication. Xiao and Gaoo [45] designed a secure 5 G authentication protocol to meet the desired objectives of third generation partnership project (3GPP). This protocol considers the standard version of 3GPP i.e., v17.4.0 to analyze a few shortcomings such as computation, communication, and storage overheads. Liu et al. [46] improved the version of the 3GPP authentication protocol to secure the essential features of session key confirmation. This improved version uses elliptic-curve Diffie-Hellman to guarantee the property of perfect forward secrecy. Braeken [47] designed a new 5 G authentication protocol based on a symmetric key to achieving anonymity and unlinkability. This symmetric key authentication optimizes the communication phases between the user equipment and home networks to enhance the performance efficiency of the networks. Yadav et al. [48] extended the 5G-AKA version of Braeken and Munilla et al. [49] to offer perfect forward secrecy and minimize the computation cost of the server database. The existing approaches [50–52] focus on the specification of 3GPP to standardize the authentication procedure between the user equipment, serving, and home networks. However, they do not have any specific strategy to keep data management services under the control of wireless base stations to process the authentication requests between the access terminals. From Table 1, we can see how significant parameters (strategy applied [33], utilized operator, security proof, applied factors [34–37], application domain [38–40], authentication with vehicle ad hoc/drone networks [53–55], and 5 G AKA [44–49]) are considered in order to examine the issues of existing authentication models [41–43].

3. Preliminaries

This section shows the typical environment of unmanned aerial vehicles and discusses the relevant security goals to meet standard constraints on central-level healthcare authorities.

3.1. Proposed architecture for military-zone surveillance

Initially, central-level authorities maintain remote servers to navigate medical emergencies and that control the pilot sites to learn the workflow required in the data maintenance process. Practical difficulties involve a heavy workload that represents the electronic information of the various geographic areas. The central authority can enlist field hospitals to offer better medical services during an outbreak of any war emergency or bioterrorism event. The field zones are inspected on a regular basis for safety. The IoMT provides several benefits, such as a collection of comprehensive data, remote monitoring, and clinical treatments that can set up preventive measures during disasters and battles. This technology can stabilize the delivery of medical services to

Table 1
Challenging issues of existing authentication models in military zones.

Existing Schemes	Applied Strategy	Utilized Operator	Security Proof	Applied Factors	Application Domain
Kalra and Sood [16]	Mutual Authentication	Elliptic-Curve Cryptography	AVISPA	Not Used	Cloud Computing
Gope and Das [35]	Mutual Authentication	XOR Operator	Theoretical	Not Used	Cloud Computing
Dey et al. [36]	Mutual Authentication	Rivest-Shamir-Adleman	Theoretical	Not Used	Cloud Computing
Gupta and Quamara [37]	Mutual Authentication	Rivest-Shamir-Adleman	AVISPA	Smartcard	Cloud Computing
Sharma and Kalra [38]	Simple Authentication	XOR Operator	AVISPA	Multi-Factor	Cloud Computing
Wang et al. [39]	Mutual Authentication	Elliptic-Curve Cryptography	ProVerif	Smartcard	Edge/Cloud Computing
Kiran et al. [29]	Mutual Authentication	Elliptic-Curve Cryptography	Theoretical	Multi-Factor	Cloud Computing
Loffi et al. [31]	Mutual Authentication	Rivest-Shamir-Adleman	AVISPA	Multi-Factor	Fog Computing
Rao et al. [30]	Simple Authentication	Not Available	Theoretical	Multi-Factor	Not Available
Zhou et al. [40]	Mutual Authentication	XOR Operator	ProVerif	Not Used	Cloud Computing
Ayub et al. [28]	Simple Authentication	Elliptic-Curve Cryptography	ROR Model	Multi-Factor	Not Available
Fan et al. [20]	Mutual Authentication	XOR Operator	BAN Logic	Smartcard	Cloud Computing
Zhang et al. [44]	Anonymous Authentication	Non-Singular Elliptic-Curve	(ROR Model	Not Used	5 G/B5G
Xiao and Gaoo [45]	5 G AKA	3GPP Specification	Strand Space Model	Not Used	5 G Wireless Networks
Liu et al. [46]		Elliptic-Curve Integrated Encryption	ProVerif	Not Used	
Braeken [47]		Symmetric Key	RUBIN Logic	Not Used	
Yadav et al. [48]			ROR, AVISPA	Not Used	
Munilla et al. [49]			Pseudo-Randomness	Not Used	
Proposed RL-SMFA	Mutual Authentication, Key Freshness, Session Key Agreement	Elliptic-Curve Cryptography	ROR	Multi-Factor	Drone Surveillance

AKA - Authentication and Key Agreement; ROR- Real Or Random; AVISPA - Automated Validation of Internet Security *Sensitive Protocol and Application.*

reduce patient wait times. Moreover, the low-cost medical infrastructure accesses medical data through wireless technology. It has the technological openness to detect several potential cyber-attacks, such as de-authentication, stepping stones, and drone-in-the-middle [56].

Data collection and processing include clinical data to examine the classification of diseases or patient conditions, which typically maintain data in formats such as Extensible Markup Language (XML) and Health Level Seven (HL7) for storage in a dedicated server system. A remote monitoring system may be automated in order to collect field data and has hospital and clinical information systems to handle the treatment process. It has a data storage table to process clinical data from a clinical trial in order to conduct logical reasoning. The major difficulty is discontinuous data that require handling of specific criteria to record a log file and remove erroneous data. However, in the data analysis, different syndrome groups are integrated to examine the chief complaints. The system may even have to deal with bioterrorism to control and prevent outbreaks, including biological disease and border threats. Intelligent aerial vehicles are openly associated with the field zones to acquire sensitive data. They can precisely locate the field zones to collect the generated packets through a wireless channel to inspect the retrieved data. The field systems have an intelligent network that connects victims through a smart device or a medical sensor to monitor their health [57].

The important parameters are blood pressure, body movement, respiration, ECG readings, heart rates, etc. These parameters are actively accessed over IoT devices like smart cameras, alarms, and motion sensors to observe the condition of the victims. In addition, users such as medical authorities may control the aerial vehicles to access confidential information via security gateway access. Fig. 3 illustrates how a military zone has four activities: aerial vehicles, smart implantable devices, wireless and gateway access, and medical authorities. Assuming medical authorities wish to determine the condition of the victims, they input a secret key to access the information via security gateways. After receiving a request, the gateway validates the secret key, and if valid, the gateway generates a random number to compute a secure session key between computing devices via the aerial network [58]. Otherwise, the gateway terminates the request.

3.2. Security goals

To achieve better security efficiency with the development of drone surveillance systems, significant key properties are briefly outlined [59, 21] as follows.

Proper user authentication: Proper mutual authentication (the so-called two-way authentication) verifies client identities with a trusted server before data are exchanged. Since a ground-based structure is sensitive in nature, the proposed RL-SMFA uses an AI-enabled secure analytics phase to verify the authenticity of aerial vehicles.

Session-key establishment: A smart intelligence system uses a systematic procedure of session key establishment to defend against man-in-the-middle attacks. As a result, the proposed RL-SMFA uses session key establishment with multi-factor authentication to secure key establishment between communication entities. Drone surveillance uses a common session key to protect privacy during data access, which can be more reliable for aerial vehicles and ensures system integrity.

No requirement for a verification table: In the proposed RL-SMFA, aerial vehicles verify system parameters such as device credentials and generate secret keys via the network gateway to resist key impersonation attacks [32]. It is worth noting that the proposed RL-SMFA does not hold any confidential information about the vehicles in the cloud server, and thus, attackers cannot perform any verification process to retrieve authentication details.

User-data freshness: Aerial sensors transmit a few forms of time-varying geographic measurements, and therefore, cannot ensure data confidentiality and integrity. To guarantee data freshness, the proposed RL-SMFA applies a request-response pair to the vehicles. In addition, it uses time synchronization to manage and secure transmissions within the network to exploit the replay attack precisely.

Anonymity: The identities of real-time entities on a public network are concealed to realize certain goals, such as being untrackable, unreachable, and non-identifiable. In other words, real-time entities disclose their identities only to trusted third parties. Therefore, the proposed RL-SMFA uses multi-factor authentication and a secure analytics phase to preserve the personal identity of the user and to secure the authentication process using hash functions.

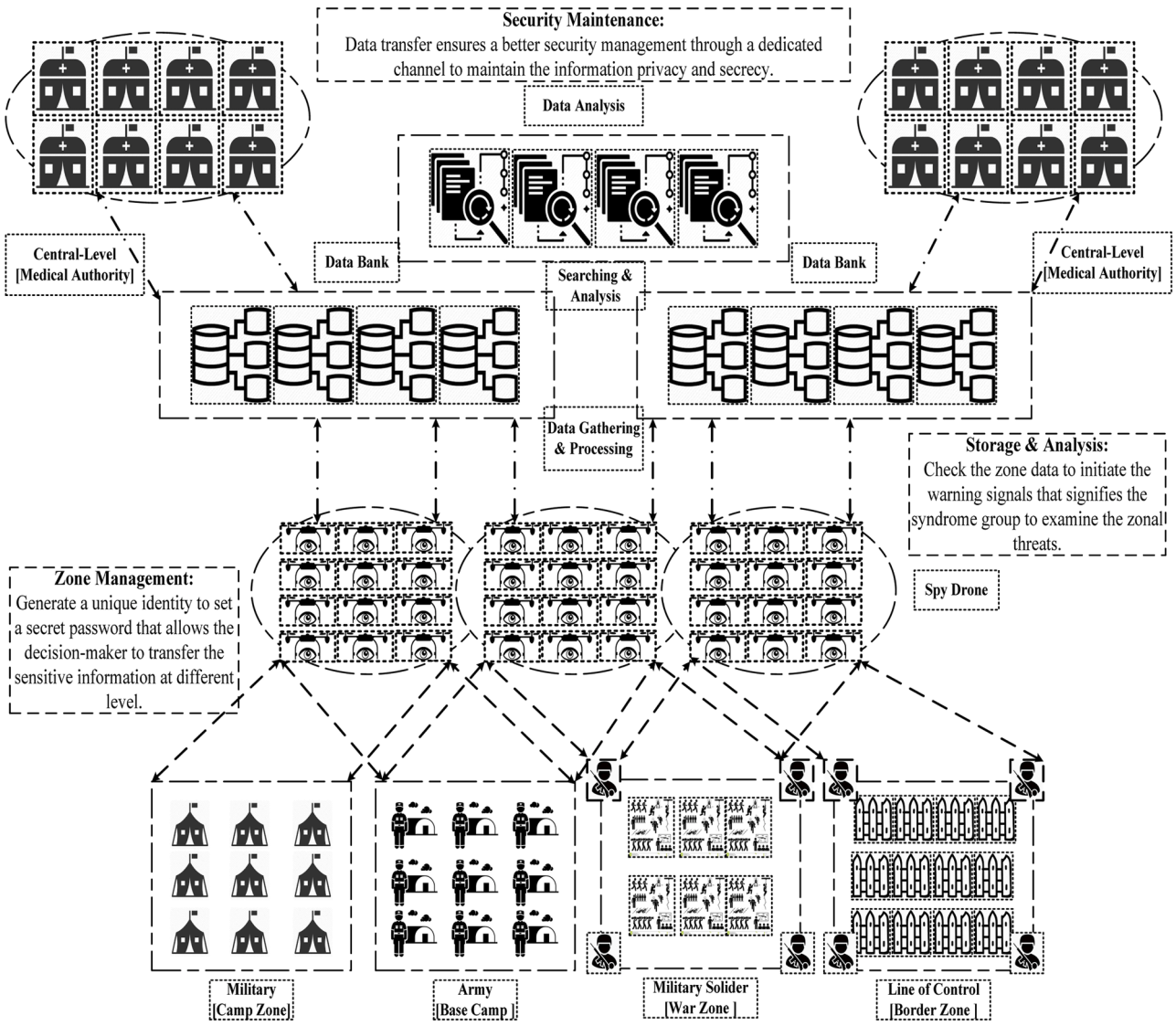

Fig. 3. Military zone surveillance for medical assistance using UAVs.

Reduced communication and computation costs: Since aerial remote sensing units have limited resources, the proposed RL-SMFA applies lightweight operators to minimize the overall cost of drone surveillance systems [61].

3.3. Mathematical primitives

The primitive considers non-singular elliptic-curve $EC_{\mathscr{p}}a,b$ to define the computation parameters over a finite-field, $\mathbb{Z}_{\mathbb{p}}$. It is defined as follows:

$$y^2 \ mod_{\mathscr{p}} \equiv x^3 + ax + b \ mod_{\mathscr{p}} \tag{1}$$

where $_{\mathscr{p}}$ is a large prime integer, $a,b \in \mathbb{Z}_{\mathbb{p}}$, and $\langle 4a^3 + 27b^2 \equiv 0 \rangle$. $G = \{x, y : x,y \in \mathbb{Z}_{\mathbb{p}} \ and \ x,y \in \ EC_{\mathscr{p}}a,b\} \cup \{\mathscr{O}\}$ creates communicative group G over addition to define the coordinates of $EC_{\mathscr{p}}a,b$. $\{\mathscr{O}_{\varepsilon}\}$ is called the *point at infinity*. The coordination points on $EC_{\mathscr{p}}a,b$ are denoted $\neq E$ in Eq. (1) to satisfy constraints such as $p + 1 - 2\sqrt{p} \leq \neq E \leq p + 1 + 2\sqrt{P}$. The basic operators are expressed as follows.

1 Assume two coordinates, $P = x_1,y_1$ and $Q = x_2,y_2$, in Eq. (1) with a specific condition, $P \neq Q$, to define the scalar addition. It is then computed as follows: $R = x_3,y_3 = P + Q$ where $x_3 = [\lambda^2 - x_1 - x_2] \ mod_{\mathscr{p}}$ and $y_3 = [\lambda^2(x_1 - x_2) - y_1] \ mod_{\mathscr{p}}$ in which λ is conditionally referred to as

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \ mod \ p, \ if \ P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \ mod \ p, \ if \ P = Q \end{cases}$$

2 Assume point P in Eq. (1) executes the sequence n times. It then computes the scalar-point multiplication as $[n.P = P + P + \ldots + P \ n \ times]$.

3 Assume point Q in Eq. (1) performs an additive inverse operation on $P = x_1,y_1$. It then computes the point-doubling operation, $[Q = 2P = P + P]$, to define an inverse image P, with respect to the given $x-axis$.

4 Assume two points, $P = x_1,y_1$ and $Q = x_2,y_2$, in Eq. (1) to express $P + Q = \mathscr{O}$, $[x_1 = x_2]$, and $[y_2 = -y_1]$. It then computes the additive inverse operation as $[P + (-P) = P - P = \mathscr{O}]$.

5 Assume coordination P can define the order of the smallest positive integer, u, to express $[u.P = \mathscr{O}]$.

3.4. Threat model

The threat model considers a valid computation strategy that defines a challenge-response game to analyze the security properties of the proposed RL-SMFA.

3.4.1. Computation models

A reliable computation strategy is formulated to validate the provable security property, which has the following computational models.

1 ***Dolev-Yao (DY)*** [62] It is assumed that A_{dv} can infer an exchange of message transmissions to explore malicious activities in terms of modifying, deleting, and inserting message contents. It is worth noting that the endpoints are not considered trusted authorities.
2 ***Ganetti-Krawczyk (GK)*** [63] It is assumed that A_{dv} can gain insecure memory access to the drone to compromise secret session keys, user credentials, and state information.

3.4.2. Assumptions

The proposed RL-SMFA uses a probabilistic polynomial time-bounded (PPT) algorithm to examine security efficiency [64]. Table 2 shows the notations used in the proposed RL-SMFA. To analyze the properties of a key agreement protocol, A_{dv} makes the following assumptions.

1 The proposed RL-SMFA has three entities (medical expert M_E, control gateway C_G, and smart drone S_D) to initiate several system instances, Π, of the given participant, PT. PT^U defines the instances of the U^{th} participant.
2 C_G has a secret session key, s_k, which authenticates M_E to hold public identity PID_j and pseudo-identity SID_j. Identities such as PID_j and SID_j are known to legal entities M_E, C_G, and S_D in order to authorize public identity ID_i and password Pwd_i. A password dictionary, P_D, is utilized to select a random integer, $|D| \leq 10^{-6}$. During the registration phase, the drone exchanges system parameters $\{F_i, Q_i, ID_i, Pwd_i, s_k\}$ and $\{PID_j, SID_j, a_j, s_k\}$ for mobile device M_D and for the memory in S_D, respectively.
3 A_{dv} considers participants M_E, C_G, and S_D to carry out any oracle query. The instances of Π may be extracted by malicious users in order to inject falsified information.
4 A_{dv} can act as an insider to access the database of C_G to extract sensitive information on session states.
5 According to the DY model, A_{dv} can exploit the instances of Π to control communication over public channels. It may eventually block or intercept the flow of transmissions between participants such as M_E, C_G, and S_D.
6 A_{dv} might obtain the secret session key of a stolen mobile device through reverse engineering to infer sensitive information such as ID_i and Pwd_i.

Table 2
Important notations used in the proposed RL-SMFA.

Notation	Description
A_{dv}	Adversary
M_E	Medical Expert
C_G	Control Gateway
M_D	Mobile Device
S_D	Smart Drone
PT	Participant
Π	System Instances
U^{th}	Participant Instance
PID_j	Public Identity
SID_j	Pseudo-identity
ID_i	User Identity
Pwd_i	Password
P_D	Password Dictionary
sk	Session Key
$H(.)$	Hash Function
$\|$	Concatenation Operator
$\oplus$	XOR Operator
$\rightarrow$	Public Channel
$\Rightarrow$	Secure Channel
ΔT	Threshold Value (i.e., for the Timestamp $1 \leq x \leq 4$)

3.4.3. Formal security proof

A_{dv} allows participant P to interact with a set of queries. It can simulate system instances Π to examine real-time attacks [65]. To compromise the key instances of Π, A_{dv} applies challenge-response game theory. As a result, A_{dv} plays a significant role in exploring the PPT algorithm. The execution steps are as follows.

- ***Execute*** $\boldsymbol{P^U}$ A_{dv} analyzes the features of passive attacks against system instances Π. If A_{dv} addresses this query, then challenger $\mathscr{C}$ issues an exchange of messages during the execution of system instances Π.
- ***Send*** $\boldsymbol{P^U, m}$ A_{dv} analyzes the features of active attacks against system instances Π. If A_{dv} reports this query to issue message transmission m from P^U, then $\mathscr{C}$ observes the transmission output to define system instances Π computed by P^U.
- ***Reveal*** $\boldsymbol{P^U}$ A_{dv} misapplies the secret session key to connect with the participants of Π. If A_{dv} reports a Reveal P^U query to $\mathscr{C}$, then $\mathscr{C}$ computes secret session key sk to accept the session between P^U and its trusted partner. Otherwise, $\mathscr{C}$ records a null value.
- ***Corrupt*** $\boldsymbol{P^U, x}$ A_{dv} corrupts a real-time participant, P^a, which obtains secret information from P^a to simulate this query. If A_{dv} executes a *Corrupt* P^U, x query, then $\mathscr{C}$ acts on the following assumptions.
  - When $x = 1$, Pwd_i of M_E is determined to be A_{dv}.
  - When $x = 2$, M_D of M_E records the storage of information.

As a consequence, A_{dv} determines session key s of C_G to execute a *Corrupt* P^U, x query. This query executes forwarding secrecy to validate the generation of a session key.

- ***Test*** $\boldsymbol{P^U}$ determines the strength of semantic security, i.e. s. A_{dv} permits $\mathscr{C}$ to issue a *Test* P^U query. If A_{dv} issues this query, then $\mathscr{C}$ determines parameter s to establish a fresh session between P^i and its trusted partner. Otherwise, it records a null value. When *Test* P^U is issued, $\mathscr{C}$ flips unbiased coin b to yield actual session key s. If $b = 1$, a random value is chosen from $0, 1^l$ for A_{dv}.

Definition 1. ***[Accepted Session State]*** We initiate a call instance to the participant P^U to verify whether the session accepts the state or not. It is cautiously preferred to analyze a message transmission that holds information on the session state authorized by the schemes.

Definition 2. ***[Trusted Partner Instances]*** We initiate two trusted partner instances, ID_i^a, V_j^b, as follows. 1. Verify whether the partners are mutually authenticated in the session state to establish a session key agreement or not. 2. Analyze whether the partners share a common pseudo-identifier, SID_j, to record a valid session identification concatenated or authorized by P^U.

Definition 3. ***[Key Freshness]*** We initiate a P^U instance to consider the key freshness property to examine the following. 1. Upon acceptance, P^U shares a common session key with trusted partners. 2. P^U or its trusted partners do not have *'No Reveal'* statement queries to process. 3. Considering P as a user instance, P^U collects a *'Corrupt-Query'* statement to process C_G information.

Definition 4. ***[Probability of Successful Events]*** Assume $Success_{Adv}^{\Pi}$ defines event states in which A_{dv} executes a *'Test Query'* not only to terminate the P^i instance against Π but to infer guess bits, $b^{'}$, as well. A_{dv}

might crack Π security semantics if $b^{'}$ equals b. It is worth noting that A_{dv} may compromise Π security semantics to express $\mathscr{A}_{Adv}^{\Pi} = Pr \| Success_{Adv}^{\Pi}| - \frac{1}{2}|$. Moreover, it uses guess a bit b to execute the *'Test Query'*.

Definition 5. ***[Semantic* Π *Security]*** Assume system authentication Π is known for semantic security if the following are true. 1. P^i and its trusted partners accept the *Adv* state in order to find a genuine session key. 2. $\mathscr{A}_{Adv}^{\Pi} \leq \varepsilon$ evaluates the genuineness of the shared session key.

4. Proposed RL-SMFA

This section considers military zone surveillance for medical assistance from UAVs using lightweight multi-factor authentication. There are six phases: server setup, drone registration, medical expert registration, system login/authentication, and secret key update. Detailed descriptions are as follows.

Phase 1. : Server Setup This phase considers a control gateway, C_G, to choose system parameters such as public and private keys to perform the following.

Step 1. Select a large prime integer, $\geq 2^{b_l}$, with an elliptic curve $EC_{\mathscr{p}}a$, b as defined by Eq. (1).
Step 2. Select a preferable basepoint, $\mathscr{P}$ of order $\mathscr{p}$, and a one-way hash function, $h : \langle 0,1\rangle^{*} \rightarrow \langle 0,1\rangle^{b_l}$.
Step 3. Select private key $pvt_k \in \mathbb{Z}_{\mathbb{p}}$ and publish system instances $\{EC_{\mathscr{p}}a, b, \mathscr{p}, \mathscr{P}, h(.)\}$.

Phase 2. : Drone Registration This registers smart drone S_{D_j} with C_G and accordingly collects system instances to authorize application services. Each registered S_{D_j} stores dedicated parameters such as ID_j and SID_j in the C_G database, which verifies the legitimacy of S_{D_j}. Steps executed by S_{D_j} and C_G are as follows.

Step 1.S_{D_j} selects secure identity ID_j and sends the identity information to C_G over a dedicated wireless channel.
Step 2. C_G validates user identity ID_j with the central database to determine whether it is unique or not. If ID_j matches any of the existing users, then C_G will notify S_{D_j} to select another identity. Otherwise, C_G chooses an integer, $a_j \in \mathbb{Z}_{\mathbb{p}}$, which is distributed uniformly to determine PID_j:

$$PID_j = h(a_j \| ID_j)$$

$$KEY_j = h(ID_j \| pvt_k \| a_j)$$

Step 3. Subsequently, C_G stores computed parameters $\{ID_j, PID_j, KEY_j\}$ in the central database. Also, it sends sensitive data $\{ID_j, PID_j, KEY_j, h(.)\}$ to S_{D_j} via a dedicated wireless channel.
Step 4. Upon receiving the information from C_G, S_{D_j} stores the values in its own secure database. **System Registration:** In this phase, a user (e.g., a medical expert/doctor) wishes to submit credentials such as identity ID_i and hashed secret key H_{sk} to the security gateway system. The user executes the following tasks.

Step 1. Select a user identity, ID_i.
Step 2. Compute system parameter $\gamma_i = H(sk_i)$.
Step 3. Accordingly, the system device sends a registration request $\{ID_i, sk_i\}$.
Step 4. Upon receiving the registration request, the security gateway executes key functions including the following:

$$\text{Compute : } \eta_i = H(ID_i.P_{\gamma_i}.P_{sk}) \oplus H(PD_K)$$

$$\text{Compute : } \alpha_i = H(\gamma_i \oplus sk_i)$$

$$\text{Compute : } \beta_i = sk_i \oplus H(I_{gd}.P_{\gamma_i}.PD_{sk})$$

Step 5. Integrate system parameters $\{ID_i, I_{gd}, H(\ .), \eta_i, \alpha_i, \beta_i, sk_i, PD_{sk}\}$ into the smart device/medical sensor.
Step 6. Establish secure communication between smart devices and smartphones through the system gateway.

System Login/Authentication: This phase invokes a system gateway when the user wishes to perform query access/data access from the medical sensor network. Fig. 4 shows the authentication phase of the proposed RL-SMFA. The execution flows are as follows.

Step 1. The smartphone/medical sensor executes computation tasks to verify the shared session key.
Step 2. It performs the following steps:

$$\text{Compute : } \gamma_i^{*} = H(sk_i)$$

$$\text{Compute : } S_K = \beta_i \oplus H(I_{gd}.P_{\gamma_i}^{*}.PD_{sk})$$

$$\text{Compute : } \alpha_i^{*} = H(\gamma_i^{*} \oplus sk_i)$$

Step 3. Verify system computation $\alpha_i^{*}? = \alpha_i$.
Step 4. In case of access failure, the smartphone/medical sensor terminates the service request to avoid security vulnerabilities.
Step 5. Otherwise, the legitimate user may gain access to compute the following:

$$D_{ID} = H(ID_i.P_{\gamma_i}^{*}.PD_K.PD_{sk}) \oplus H(pvt_k.PT_m)$$

$$\varepsilon_i = H(\eta_i.PD_K.PD_{sk}.PT_m)$$

The user (e.g., a medical expert/doctor) issues a login request $\{D_{ID}, \varepsilon_i, PD_K, PT_m\}$ through the system gateway.

Step 6. Upon receiving the login request, the gateway executes the following:

$$\text{Verify : } PT_{m1} - PT_m \leq \Delta_T$$

Step 7. If verification is unsuccessful, the gateway aborts the service request.
Step 8. Otherwise, the gateway executes the following:

$$\text{Compute : } \zeta^{*} = D_{ID} \oplus H(pvt_k.PD_K.PT_m)$$

$$\varepsilon_i^{*} = H(\zeta^{*} \oplus H(PD_K)PD_{sk}.\ PT_m)$$

$$\text{Verify : } \varepsilon_i^{*}? = \varepsilon_i$$

Step 9. If verification is unsuccessful, the gateway aborts the login request.
Step 10. Otherwise, the system gateway computes $\sigma_i = H(D_{ID}.PD_{sk}.PD_K.PT_{m1})$.
Step 11. The gateway sends system parameters $\{D_{ID}, \sigma_i, PD_K, PT_{m1}\}$ to the medical sensor/smartphone.
Step 12. After receiving the request message, $\{D_{ID}, \sigma_i, PD_K, PT_{m1}\}$, the medical sensor/smartphone executes the following task:

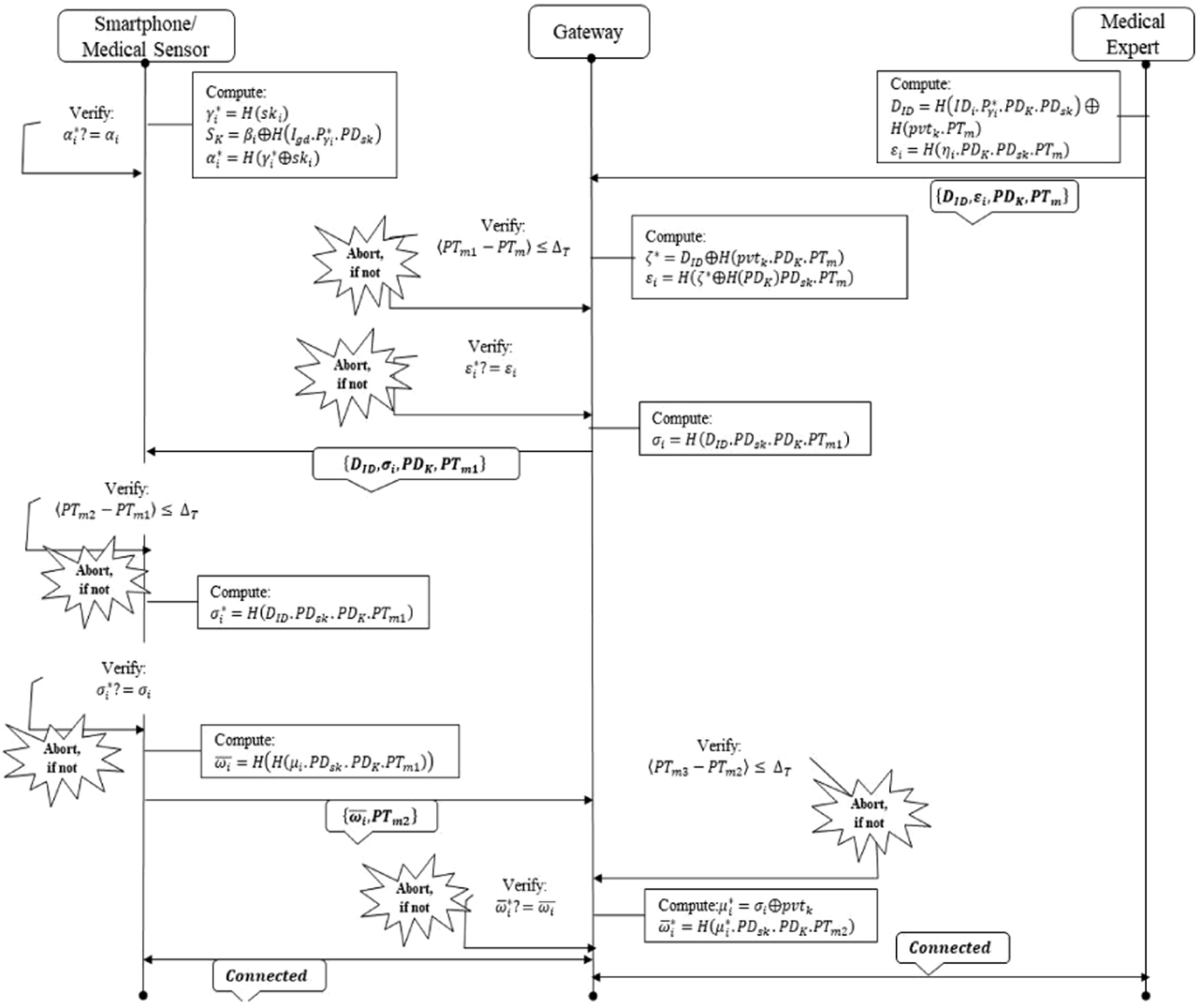

Fig. 4. System authentication phase.

Verify : $PT_{m2} - PT_{m1} \leq \Delta_T$

Step 13. If verification is unsuccessful, the smartphone/medical sensor aborts the process.
Step 14. Otherwise, it computes $\sigma_i^* = H(D_{ID}.PD_{sk}.PD_K.PT_{m1})$ to verify whether the expression $\sigma_i^* ? = \sigma_i$ holds or not.
Step 15. If verification is unsuccessful, the smartphone/medical sensor aborts the request.
Step 16. Otherwise, it computes $\overline{\omega_i} = H(H(\mu_i.PD_{sk}.PD_K.PT_{m1}))$ to send system parameters $\{\overline{\omega_i}, PT_{m2}\}$ to the gateway. Then, the gateway executes the following to ensure system privacy:

Verify : $PT_{m3} - PT_{m2} \leq \Delta_T$

Step 17. If verification is unsuccessful, the gateway aborts the process.
Step 18. Otherwise, it computes $\mu_i^* = \sigma_i \oplus pvt_K$ and $\overline{\omega}_i^* = H(\mu_i^*.PD_{sk}.PD_K.PT_{m2})$ to verify whether $\overline{\omega}_i^* ? = \overline{\omega_i}$ holds or not.
Step 19. If verification is successful, the gateway sends an acceptance message to the medical sensor/smartphone. Otherwise, it terminates the request.

After receiving the acceptance message, the medical sensor/smartphone responds to the user queries of the medical expert/doctor.

Secret Key Update: In the proposed RL-SMFA, the secret key of a legitimate user can be changed without the gateway to reduce computation and communication overhead. During a secret key update, a registered user can change the secret key when he/she needs to. The secret key update is concurrently reflected in the system database to ensure seamless connectivity between the smartphone and the medical sensor. This strategy is more useful in mitigating the problem of scalability and in facilitating user-friendliness.

After receiving a new secret key s_k^{New}, the smartphone/medical sensor confirms its validity using $\alpha_i^* ? = \alpha_i$. If the condition is valid, the smartphone/medical sensor computes new parameters $\{\eta_i^{New}, \alpha_i^{New}, \beta_i^{New}\}$ and updates those parameters. Otherwise, the smartphone/medical sensor aborts the update request. The user generates input such as $\{ID_i, s_{k_i}, s_{k_i}^{New}\}$ for the smartphone/medical sensor.

The smartphone/medical sensor performs the following task to ensure system fidelity.

It computes $\gamma_i^* = H(s_{k_i})$ and $s_k = \beta_i \oplus H(I_{gd}.PD_{sk}.PD_K.P_{\gamma_i}^*)$ to verify whether $\alpha_i^* = H(\gamma_i^* \oplus s_k) ? = \alpha_i$ holds or not.

In addition, it computes $\eta_i^{New} = \eta_i^{New} \oplus H(I_{gd}.PD_{sk}.PD_K.P_{\gamma_i}) \oplus H(I_d.PD_K.H(s_{k_i}^{New}).PD_{sk})$, $\alpha_i^{New} = H(H(s_{k_i}^{New}) \oplus s_k)$, and $\beta_i^{New} = s_k \oplus H(I_{gd}.PD_K.H(s_{k_i}^{New}))$ to replace old key parameters $\{\eta_i, \alpha_i, \beta_i\}$ with $\{\eta_i^{New}, \alpha_i^{New}, \beta_i^{New}\}$

Therefore, smart devices like smartphones/medical sensors have new values, namely $\{\eta_i^{New}, \alpha_i^{New}, \beta_i^{New}\}$, to re-authenticate system phases, including login and authentication. The system phases use symmetric key-based encryption to resist physical node capture attacks and have fewer computational resources on smart drone S_D to minimize infrastructure costs deployed by the surveillance systems. In this system, the proposed SMFA adheres to the property of saveless key management and session key negotiation between the smart devices via a gateway to resist secret data leakage. Most importantly, the proposed SMFA adopts a service scenario of mutual authentication to formulate the design goals of the 5 G standard including bandwidth, latency, and reliability to build a surveillance network with improved data transmission efficiency.

AI-Enabled Secure Analytics: This phase prevents a data poisoning attack that injects fake data from a malicious user. As a result, it might alter the training dataset to confuse artificial intelligence or machine learning algorithms. Moreover, a crucial factor in this attack is to diagnose the execution parameters of aerial images, such as $\{Cmd_{CS,S_D}, Data_{C_G,M_E}, Req_{M_D,C_G}\}$. It uses an authentication system property to validate the genuineness of system entities like S_D and M_D, and applies learning approaches to analyze prediction accuracy. The execution is detailed in Algorithm 1. Since data privacy is harder to enforce limitations in state-of-the-art of cryptography, the B5G network focuses on data analytics to mask user-specific information. The emerging network applies a learning framework to generalize the specific weighted parameters using AI and predict the appropriate features managed by healthcare authorities to exchange mobile data with the user via the cloud explicitly. Lastly, the healthcare authorities use a proactive learning approach to discover specific features related to medical screening and surveillance to accelerate learning accuracy with privacy preservation.

5. Security analysis

This section discusses the important features of session key agreements to guarantee data confidentiality, integrity, and mutual authentication. In the proposed RL-SMFA, lightweight operators are preferred not only to minimize cost efficiencies but also to recover a few secret values to compare security efficiencies of drone surveillance systems [66]. To validate the security requirements of the surveillance systems, both formal and informal approaches are applied.

Algorithm 1
Data verification using AI.

Input *A pool of data transactions has N commands to analyze malicious activities, where N is the execution commands between S_D/M_D and C_G.*
Output *Consider a fake node F_N and false data F_D to examine operations including commitment and addition.*
Assume the verifier known as the control gateway C_G elects a round-robin strategy to analyze the falsified data.
C_G gathers real-time data securely from the database pool and generates system command Cmd_x
C_G broadcasts Cmd_x to the available S_D/M_D to record aerial images over a dedicated wireless channel.
C_G validates the aerial images from the database to verify the genuineness of S_D/M_D.
for each control gateway C_G do
  use timestamp T_P to verify the current hash value.
  upon successful verification, the hash values are broadcast to the central database
end for
Consider Val to be a valid response to initialize Val→0.
for each committed message in a central pool
do
  C_G computes Val
  if such a committed message is valid then
    Set Val→Val + 1
  end if
end for
if $(Val > 2F_N + 1)$ then
  Broadcast the blocked message to a trusted partner C_G
  Add Cmd_x into S_D/M_D
end if

5.1. Analysis I: formal approach

In this section, provable security is constructed using the PPT algorithm to solve the computational Diffie-Hellman assumption problem.

***M_E* Security*Provable Security*:** Let us assume that A_{dv} wishes to derive a secret parameter b. In order to determine b, A_{dv} executes a test query via proper guessing bit b' associated with parameter b. Upon query execution, A_{dv} tries to issue a fresh test case to find the transmitted bit b from the random oracle model, π_U^i. In case of successful execution, A_{dv} may interrupt the session key of M_E protocol P to gain user access. Hence, the probability of A_{dv} winning a game is $P_r[b' = b]$. In brief, adversary Eve Adv_{Eve} associated with protocol attack P_A can be defined as $Adv_{P_A}^{AKE}(E_{ve}) = |2 \times P_r[b' - b] - 1|$ to retrieve user credentials. More precisely, P_A represents a security factor of M_E, whereas $Adv_{P_A}^{AKE}$ is negligible while recovering significant secret values of b.

Theorem 1. *Let us say that Adv_{Eve} is an adversary of smart computing devices with query execution time $T_{Adv_{Eve}}$, which requires lower execution cost Q_S over the communication entities as well as a hash function Q_{hash} to acquire security parameters M_E of the proposed RL-SMFA. Therefore, the execution cost can be defined as $Adv_{P_A}^{AKE}[Adv_{Eve}, Q_S, Q_{hash} \times Success\prod_{Adv} T'_{Adv_{Eve}}]$ where $T'_{Adv_{Eve}}$ denotes the successful computation time ($Success\prod_{Adv}$), and $Q_S = \sum_{i=1}^{4} Q_{S\_I}$ shows a summation of the query execution, i.e., $Send_1$, $Send_2$, $Send_3$, and $Send_4$.*

Proof of Theorem 1**:** We assume that Adv_{Eve} is an attacker or adversary trying to acquire a security factor ε to extract confidential parameters of M_E within the stipulated query execution time, $T_{Adv_{Eve}}$. To inspect the extraction process, the query processing system $\prod$ may launch a passive attack, i.e., P_{ATT}, to deal with the Adv_{Eve} query responding to trusted partners ID_i^a, V_j^b where P_{ATT} challenges $\nu \geq 2^{b_l}$ to issue $pvt_k \in \mathbb{Z}_{\mathbb{p}}$ with elemental output $\mathbb{Z}$.

Basically, Adv_{Eve} executes $Send_1$ to initiate the query process that later relies upon the intention of P_{ATT} to issue a transmission $Msg_1 ID_j$, $PID_j, KEY_j, h(.)$ to Adv_{Eve}. Accordingly, when Adv_{Eve} processes a $Send_2$ query, P_{ATT} randomly chooses two prime integers, c_1 and c_2, from a cost function $1, Q_{S\_2}$. If $c_1 \neq c_2$, P_{ATT} replies with $Msg_2 ID_i, I_{gd}, H(.), \eta_i, \alpha_i, \beta_i, sk_i$, PD_{sk} to Adv_{Eve}. Otherwise, P_{ATT} utilizes $\aleph$ to consolidate a few communication parameters of g^k that subsequently apply to $Msg_2 ID_i, I_{gd}, H(.), \eta_i$, α_i, β_i, sk_i, PD_{sk} in order to compute new message transmission Msg_2' associated with Adv_{Eve}.

While obtaining query $Send_3$ from Adv_{Eve}, P_{ATT} replies with message transmission $Msg_3 D_{ID}, \sigma_i, PD_K, PT_{m1}$ to execute constructive steps in the proposed RL-SMFA. If construction is successful, P_{ATT} uses $\aleph's$ query input to compute a new message transmission, Msg_3', and updates the transmitted parameters with Adv_{Eve}. Lastly, P_{ATT} execute a $Send_4$ query to return a string value *NULL*. Hence, it is shown that the proposed RL-SMFA can be successful in executing all the set conditions.

On the other hand, while issuing an oracle model *Reveal* π_U^i or *Reveal* $\pi_{SK_j}^i$ from Adv_{Eve}, P_{ATT} checks whether the execution of the oracle model is successful or not in order to define key freshness with the encrypted message transmission. If verification is successful, P_{ATT} can infer a predetermined session key between a legitimate device $S_{K(i,j)}$ and Adv_{Eve}. Otherwise, P_{ATT} aborts the query assuming that the session key of the legitimate devices cannot be determined from $\aleph$. Likewise, while issuing the oracle queries *Corrupt* M_E, *Corrupt* C_G, *Execute* π_{UA}^i, π_{UB}^i, and *Hash Msg* from Adv_{Eve}, P_{ATT} honestly replies to all executed queries. If not, the session key of the legitimate device from P^U is determined to be new, and thus, P_{ATT} shares the random string with Adv_{Eve} to compute a session key $S_{K(i,j)}$.

From the above assumption, it is claimed that the proposed execution

protocol PE_P may be indispensable in analyzing metrics such as session state, trusted instance, and key freshness, except those involving $P^U = ID_j, PID_j, KEY_j$. Let us assume that for a given probability γ, P_{ATT} tries to guess the session key of the legitimate devices. It uses query model $Test\ \pi_U^i$ to confirm whether $\overline{\omega}_i^* ? = \overline{\omega_i}$ or not. Hence, P_{ATT} has a probability of success $\gamma = 1/Q_{S\_2} \geq 1/Q_S$ for computing the actual session key.

To validate the above query model $Test\ \pi_U^i$, Adv_{Eve} declares output query $b^{'}$. As a result, this model verifies whether $b = b^{'}$ in order to find the session key of the legitimate devices using *Hash Msg*. For given probability λ, the hash query model may be defined as $\lambda \geq 1/Q_H$. Also, the probability of success $Succ_G^{CDH} P_{ATT}$ that P_{ATT} exposes $\mu_i^* = \sigma_i \oplus pvt_k$ challenging P^U can be expressed as $Success_{Adv}^{\Pi} A_{TT} = \varepsilon \times \gamma \times \lambda \geq \varepsilon \times (1/Q_S) \times (1/Q_{hash})$. Lastly, the possibility of Adv_{Eve} breaking A_{KE} security is $\varepsilon = \mathscr{A}_{A_{dv}}^{\Pi} Adv_{Eve}, Q_S, Q_{hash} \leq Q_S Q_{hash} \times Success_{Adv}^{\Pi}(T_{ADeve}^{'})$.

5.2. Informal analysis

In this section, a few security attributes of key agreement protocols are analyzed to prove the efficiency of the proposed RL-SMFA over other schemes.

Stolen Smart Device or Medical Sensor: Let us assume that a smart computing device is snatched or pirated; then, *Adv* has a chance to extract user credentials $\{\eta_i^{New}, \alpha_i^{New}, \beta_i^{New}\}$ using a strategic attack known as a side channel (or invasive) attack. Accordingly, *Adv* may use the extracted information to compute a legal session key to impersonate the trusted device. In real time, *Adv* tries to access the extracted information via the gateway; however, *Adv* might not generate a genuine login request, i.e., $\{D_{ID}, \sigma_i, PD_K, PT_{m1}\}$. Since *Adv* cannot determine computed values $D_{ID}, \varepsilon_i, PD_K$, and PT_m, $\{\gamma_i, s_{k_i}\}$ might not be identified in order to find the identity of the device. Thus, the proposed RL-SMFA can be resilient to a stolen smart-device/medical-sensor attack.

Security Gateway Impersonation: Assume A_{dv} uses a node capture attack to interfere with confidential information in computing devices $\{PD_K, s_k\}$. As a consequence, A_{dv} can access a login request such as $PT_{m1}.\{D_{ID}, \varepsilon_i, PD_K, PT_m\}$ and $PT_{m2}.\{D_{ID}, \varepsilon_i, PD_K, PT_m\}$ to overhear device communications at any time. However, A_{dv} cannot tamper with the system values of the previous login request, such as $H(I_d.P_{\gamma_i}.PD_K)$, because the computed value of γ_i varies over parameter *sk*. Thus, the proposed RL-SMFA can prevent A_{dv} from exploiting a node capture attack to infer key credentials and impersonate a control gateway.

Forgery with Node Capture: Let us say that A_{dv} wishes to tamper with system parameter $\{PD_K, S_K\}$ using a node capture attack. Unfortunately, A_{dv} cannot form a legal login message $\{\overline{\omega}_i, PT_{m2}\}$ to impersonate a legitimate device owing to the fact that μ_i might not be assessed until the value of σ_i is determined. Thus, the proposed RL-SMFA prevents A_{dv} from exploiting a node capture attack to forge the confidential value of σ_i.

Password-Guessing: Since the control gateway and smart computing device or medical sensing units do not maintain a verifier table or a password database, the proposed RL-SMFA proves that A_{dv} cannot exploit external entities to validate guessed information, e.g., an encryption key.

Security Gateway Bypass: Since the system parameter *sk* is not collected in any of the sensing units or computing devices, A_{dv} cannot use any subnets of a heterogeneous network to support communication via the control gateway. Also, without accessing the control gateway, system parameters like $D_{ID}, \varepsilon_i, PD_K$, and PT_m cannot be obtained. More importantly, smart computing devices or medical sensing units cannot write a system query until the control gateway processes a legal login request. Thus, under the proposed scheme, A_{dv} cannot use conversion code to launch gateway bypass attacks.

Insider Attack: In the proposed RL-SMFA, secure hash key $\gamma_i = H(sk_i)$ initiates system registration to compute *sk*. In real time, *Adv* tries to obtain $\alpha_i = H(\gamma_i \oplus sk_i)$ and $\beta_i = sk_i \oplus H(I_{gd}.P_{\gamma_i}.PD_{sk})$ to intercept the login request. However, A_{dv} cannot obtain γ_i because the computed value of γ_i varies over parameter *sk*. Hence, the proposed RL-SMFA can be resilient to node capture and insider attacks.

Resilience to a Known Session-key Attack: The proposed RL-SMFA applies $s_k = \beta_i \oplus H(I_{gd}.PD_{sk}.PD_K.P_{\gamma_i}^*)$ to investigate specific parameters like β_i and I_{gd}. It has a session-specific strategy to examine whether A_{dv}can obtain the current session key upon substitution of the old session records. In other words, even if A_{dv} obtains the old session records, he/she cannot infer the current session key of any legal entity. Hence, the proposed RL-SMFA is resilient to the known session-key attack.

Resilience to a Drone Impersonation Attack: In the authentication phase, system parameters like $D_{ID} = H(ID_i.P_{\gamma_i}^*.PD_K.PD_{sk}) \oplus H(pvt_k.PT_m)$ and $\varepsilon_i = H(\eta_i.PD_K.PD_{sk}.PT_m)$ are utilized to determine whether real-time entities such as M_E/M_D and S_D are genuine or not. Similarly, instances such as $\zeta^* = D_{ID} \oplus H(pvt_k.PD_K.PT_m)$ and $\varepsilon_i = H(\zeta^* \oplus H(PD_K)PD_{sk}.\ PT_m)$ are computed to verify whether the control gateway C_G is an authorized partner or not. As a result, A_{dv} cannot be authorized as a legitimate entity or partner, proving that the proposed RL-SMFA is resilient to drone impersonation attacks.

Acquisition of Anonymity and Untraceability: A_{dv} tries to monitor system instance $\{ID_j, PID_j, KEY_j, h(.)\}$. However, A_{dv} cannot infer or overhear the transmission of data between S_D/M_D and C_G in plaintext form. As a result, the proposed R-LMFA can attain anonymity. Moreover, the transmitted messages entertain a unique identity, which is not only for exchanging session keys dynamically but is also used to authenticate sessions of S_D. Therefore, A_{dv} cannot trace any message transmission between S_D/M_D and C_G, preserving untraceability.

Provision for a Zero-Knowledge Password: Because the proposed RL-SMFA restricts disclosure of the session key with registered computing devices or sensing units via the control gateway, it may allow the devices to authenticate a key verifier in order to protect sensitive information in the computing domains.

Mutual Authentication for Smartphone/Medical Sensor Gateway Access: Since the proposed RL-SMFA cannot exploit a node capture attack to forge the confidential value of σ_i, it can be more realistic to maintain proper mutual authentication between sensing components such as S_D/M_D and control gateway C_G.

6. Performance analysis

This section analyzes the performance of the proposed RL-SMFA compared to other schemes to examine five cost factors: signaling, communication, computation, storage, and energy.

6.1. Analysis I – signaling cost

In this analysis, the message transmission rounds are chosen to examine the signaling cost efficiency of the proposed RL-SMFA and other related authentication schemes. Most real-time applications use cloud and edge computing systems to verify the reliability of secure and common channels [67] which mainly include hashing $H(\ )$, exclusive operator $X-OR(\ )$, concatenation $con(\ )$ to generate a session key between the smart devices via a trusted gateway. The application initializes various computing events namely capture, authenticate, and control to establish secure communication. In order to evaluate the computing events, authentication and key agreement mechanism mutually exchange the communication with various core elements. The key agreement mechanisms include the signaling message to compute the cost efficiency of the proposed RL-SMFA and other existing mechanisms. In the proposed RL-SMFA, the authentication phase consumes three message rounds between the medical devices and the experts via gateway access.

Lwamo et al. [41] use five transmission rounds to execute challenge-response methods in a multi-server environment. Azrour et al.

[42] execute four request and response messages to interact with medical sensing units in real time. Bagga et al. [43] mutually exchange four transmission rounds to accomplish secure data access with IoT devices. Ma et al. [53] generate four transmission requests to realize mutual authentication with fog-based vehicular ad hoc networks (VANET). Gope and Sikdar [54] operate five challenge-response methods to establish a secure session key with privacy preservation for edge-assisted Internet of Drone (IoD). Ever [55] employs four transmitted message requests to assess the effectiveness of the security framework for IoD applications. Koutsos [50] requires six transmission rounds to exchange communication with the core networks and communication terminals. Fan et al. [51] consume five message requests to access the terminals via a dedicated core network in accordance with the specification of 3GPP. Cao et al. [52] have three message rounds to complete the process of key authentication and negotiation with the core network which makes the terminals to exchange communication securely. While analyzing the key agreement phase, the proposed RL-SMFA consumes less signaling cost than other existing schemes [41–43,50–55] to improve the robustness of session key security.

6.2. Analysis II – communication cost

As mentioned in [48], the output sizes of the hash function, timestamp, and symmetric encryption/decryption are 20 *bytes*, 4 *bytes*, and 16 *bytes*, respectively. In addition, a one-point multiplicative group G and G_1 are 40 *bytes* and 128 *bytes*. Table 3 shows the communication efficiencies of the proposed RL-SMFA compared with other schemes [41–43,50–55]. Execution phases like login and authentication are preferred when analyzing message rounds to compute the communication costs of the proposed RL-SMFA and other authentication schemes [41–43,47–49].

Ma et al. [53] had four message rounds during system login and authentication, which are as follows: $|A_{ID_U}, T_{U_i}, R_1, \alpha| = 20 + 4 + 40 + 20 = 84$ *bytes*, $|A_{ID_U}, A_{ID_{FN_j}}, T_U, T_{FN}, R_1, R_2, \widetilde{R_2}, \alpha, \beta| = (20 \times 4) + (4 \times 2) + (40 \times 3) = 208$ *bytes*, $|R_3, \widetilde{R_3}, R_3^{'}, T_{CS}, \gamma, \overline{\gamma}| = (40 \times 3) + (4) + (20 \times 2) = 164$ *bytes*, and $|R_2, \widetilde{R_3}, R_3^{'}, T_{CS}, \overline{\gamma}| = (40 \times 3) + (4) + (20) = 144$ *bytes*. The total communication overhead for Ma et al. [44] was $84 + 208 + 164 + 144 = 600$ *bytes*. Gope and Sikdar [54] consumed five message rounds during authentication as follows: $|PID_u^i, FID| = 40$ *bytes*, $|A_{ck}, ID_{MEC}| = 20 + 20 = 40$ *bytes*, $|P_{ID}^i, N_U, ID_{MEC}| = 20 + 4 + 20 = 44$ *bytes*, $|PID^*, N_S, C_i, R_{Server}| = (20 \times 2) + (4 \times 2) = 48$ *bytes*, and $|R_{i+1}^{x^*}, R_{i+1}^{y^*}, R_{UAV}, E_L| = (20 \times 3) + 40 = 100$ *bytes*. The total communication overhead for Yadav et al. [48] was $40 + 40 + 44 + 48 + 100 = 272$ *bytes*.

Ever [55] had four message rounds during system login and authentication: $|PID_{MS}, b_j, c_j, N_j| = (40 \times 2) + (20 \times 2) = 120$ *bytes*, $|PID_{MS}, x, SK_{MS}, N_j, s, PK, LCH_{DB}| = (20 \times 5) + (4) + (16) = 120$ *bytes*, $|TS_S, PID_j, x, SK_j, Certify_j, CH_{ID_j}| = (4) + (40 \times 4) + 16 = 180$ *bytes*, and $|CH_{ID_j}, S_{k1}, PID_j, TS_S| = 40 \times 4 = 160$ *bytes*. The total communication overhead for Ever [55] was $120 + 120 + 180 + 160 = 580$ *bytes*. Lwamo et al. [42] comprised four rounds of transmitted messages to establish secure interaction with the medical sensing units: $|V_1, MID, A, ID_{SN}, T_1| = (40) + (20 \times 3) + 4 = 104$ *bytes*, $|V_2, B, MID, T_2| = (20 \times 3) + 4 = 64$ *bytes*, $|V_3, C, HID, ID_{SN}, T_3| = (20 \times 4) + 4 = 84$ *bytes*, and $|V_4, D, ID_{SN}, T_4| = (20 \times 3) + 4 = 64$. The cost efficiency of Lwamo et al. [41] was $104 + 64 + 84 + 64 = 316$ *bytes*. The other authentication schemes, namely, Bagga et al. [43] and Zhang et al. [44], typically utilized the above strategy to find efficiency factors as follows: $(9 \times 20) + 40 + (6 \times 16) = 316$ *bytes* and $(132) + (216) + (100) + (68) = 516$ *bytes*, respectively.

The proposed R-LMFA requires three message rounds during login and authentication: $|D_{ID}, \varepsilon_i, PD_K, PT_m| = 20 \times 4 = 80$ *bytes*, $|D_{ID}, \sigma_i, PD_K, PT_{m1}| = 20 \times 4 = 80$ *bytes*, and $|\overline{\omega_i}, PT_{m2}| = 20 \times 2 = 40$ *bytes*. The total cost of the proposed RL-SMFA is $80 + 80 + 40 = 200$ *bytes*. Koutsos [50] consumed six transmission rounds such as $\{sup_i, sqn_u, mac_{km}, pk_n, n_r\}$, $\{mac_{km}, sqn_r, n_j\}$, $\{guti_{id}, b_{id}, session_{id}, b - auth_j\}$, $\{n_j, sqn_{id}, f_{kid}, mac_{km}, guti_{id}\}$, $\{b_{id}, mac_{km}, n_r\}$, and $\{guti_{id}, f_{kid}, mac_{km}, n_j\}$ to obtain $20 \times 8 + 40 \times 4 = 320$ *bytes*. Fan et al. [51] executed five transmission rounds such as $\{sup_i, R, pk\}$, $\{xres, k, rand\}$, $\{ck, k, rand, ik\}$, $\{autn, sqn, ak, manc\}$, and $\{ak, k, rand, mac\}$ to gain $20 \times 6 + 40 \times 8 = 440$ *bytes*. Cao et al. [52] obtained three message rounds such as $\{ID_{SN}, T_x, K_{sn}, p, E_1, MAC_1\}$, $\{ENC_K, T_y, K_{sn}, p, K_{ue}, MAC_2\}$, and $\{MAC_3\}$ to attain $20 \times 4 + 40 \times 5 + 4 \times 2 = 288$*bytes*. From Fig. 5, we can see that the proposed RL-SMFA consumes 200 *bytes* during system login and authentication, whereas the other schemes [41–43,50–55] require 600 *bytes*, 272 *bytes*, 580 *bytes*, 360 *bytes*, 316 *bytes*, and 516 *bytes*. The comparative analysis shows that the proposed RL-SMFA has a lower communication cost than the other authentication schemes, improving transmission and routing efficiency.

Table 3
Communication efficiencies of the proposed RL-SMFA and other schemes.

Authentication schemes	Message rounds	Communication cost *bytes*
Ma et al. [53]	4	600
Gope et al. [54]	5	272
Ever [55]	4	580
Azrour et al. [42]	4	360
Lwamo et al. [41]	5	316
Bagga et al. [43]	4	516
Koutsos [50]	6	320
Fan et al. [51]	5	440
Cao et al. [52]	3	288
Proposed RL-SMFA	3	200

6.3. Analysis II: computation cost

As mentioned in [49], the proposed RL-SMFA and other existing schemes incur computation overhead. A dedicated notebook was employed for analysis of computation efficiencies; it was powered by an Intel Core i-7 @ 3.4 GHz with 16GB of RAM, had a 1 TB HDD, and ran Ubuntu Linux 20.04 LTS for the cryptographic operation of approximately 5000 *times*. It rendered average execution times based on the availability of the MiRACL library [68]. Assume $T_{BP} \approx 4.211$ *ms*, $T_{BP(M)} \approx 1.709$ *ms*, $T_{TP(M)} \approx 4.406$ *ms*, $T_{EM} \approx 0.442$ *ms*, $T_H \approx 0.0001$ *ms*, $T_A \approx 5.93$ *ms*, and $T_{ED} \approx 0.0026$ *ms* represent bilinear pairing, bilinear

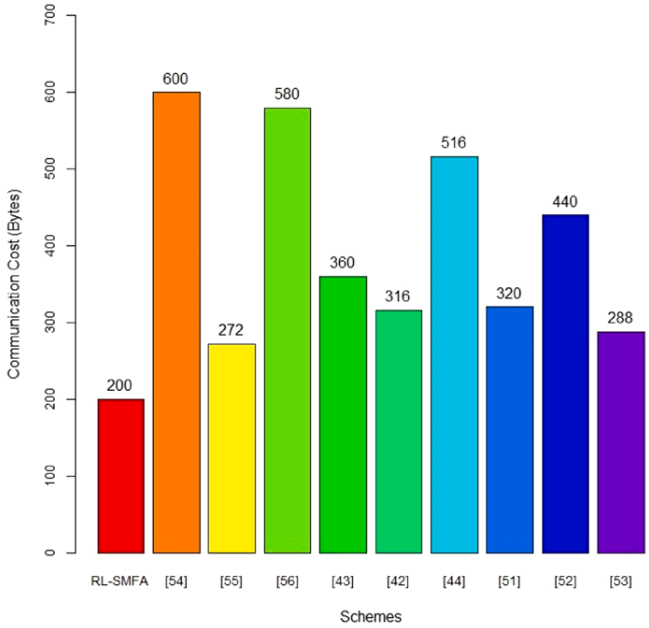

Fig. 5. Comparison of communication overhead (*Bytes*).

pairing (multiplication), map-to-point hashing, elliptic-curve cryptography (multiplication), one-way hashing, modular addition, and symmetric encryption/decryption, respectively. It is worth noting that bitwise XOR was ignored because it is less expensive than other operators. To analyze the primitive characteristics of the proposed RL-SMFA and other existing schemes [41–43,50–55], a detailed analysis includes login, authentication, and key agreement phase.

The proposed RL-SMFA utilizes 3 elliptic-curve multiplication and 4 bilinear one-way hashing to complete the message request of the smart object whereas the drone/aerial vehicle and trusted gateway require 14 elliptic-curve multiplication and 15 bilinear one-way hashing respectively to establish a secure communication using authentication and key agreement phase. As a result, the total computation cost of the proposed RL-SMFA is estimated to be $17T_{EM} + 19T_H \approx 7.51$ *ms*. Lwamo et al. [41] necessitate $17T_H + 16T_{EM} + 17T_{ED} \approx 7.11$ *ms* to authenticate the computing services provided by multi-server design whereas Azrour et al. [42] require $17T_H + 5T_{EM} \approx 2.21$ *ms* to guarantee the cost efficiency of remote healthcare systems. Bagga et al. [43] use $26T_H + 10T_{EM} + 1T_{ED} \approx 4.43$ *ms* to access the IoT devices vi a high-scale network to show its practical applicability. Ma et al. [53] consume $17T_{EM} + 19T_H \approx 7.51$ *ms* to achieve good computation efficiency with interconnected vehicles and edges. Gope et al. [54] operate $2T_{EM} + 2T_A + 3T_H \approx 12.74$ *ms* to ensure efficient network operation with better service delivery. Ever [55] consumes $6T_{BP} + 17T_H + 4T_{EM} \approx 27.03$ *ms* to achieve high-level computation requirements including energy and bandwidth. Koutsos [50] reserves $5T_H + 2T_A \approx 11.86$ *ms* to establish to guarantee better privacy with efficient design constraints. Fan et al. [51] make $3T_H \approx 0.0003$ *ms* to achieve distributed authentication with stronger security. Cao et al. [52] utilize $2T_H + 2T_{ED} + 5T_{BP(M)} \approx 8.55$ *ms* to establish secure communication with the core network and IoT terminals.

Table 4 shows the computation efficiencies of the proposed RL-SMFA and the other schemes [41–43,50–55]. Comparative results show that the proposed RL-SMFA consumes less computation overhead than related schemes [41,43,50,52–55] except for Azrour et al. [42] and Fan et al. [51] as shown in Fig. 6.

6.4. Analysis IV: bandwidth consumption

In this analysis, bandwidth overhead considers the transmitted message sizes of the proposed RL-SMFA and other existing schemes

Table 4
Computation efficiencies of the proposed RL-SMFA and other schemes.

Schemes	Smart Object	Drone/ Aerial Vehicle	Trusted Gateway	Total Cost
Ma et al. [53]	$3T_{EM} + 4T_H$	$4T_{EM} + 4T_H$	$10T_{EM} + 11T_H$	$17T_{EM} + 19T_H \approx 7.51$ *ms*
Gope et al. [54]	Not Available	$1T_{EM} + 1T_A + T_H$	$1T_{EM} + 1T_A + 2T_H$	$2T_{EM} + 2T_A + 3T_H \approx 12.74$ *ms*
Ever [55]	$2T_{BP} + 5T_H$	$2T_{BP} + 3T_H$	$2T_{BP} + 9T_H + 4T_{EM}$	$6T_{BP} + 17T_H + 4T_{EM} \approx 27.03$ *ms*
Azrour et al. [42]	$6T_H + 2T_{EM}$	$8T_H + 3T_{EM}$	$5T_H$	$17T_H + 5T_{EM} \approx 2.21$ *ms*
Lwamo et al. [41]	$17T_H + 16T_{EM} + 17T_{ED}$			≈ 7.11 *ms*
Bagga et al. [43]	$26T_H + 10T_{EM} + 1T_{ED}$			≈ 4.43 *ms*
Koutsos [50]	$5T_H + 2T_A$			≈ 11.86 *ms*
Fan et al. [51]	$3T_H$			≈ 0.0003 *ms*
Cao et al. [52]	$2T_H + 2T_{ED} + 5T_{BP(M)}$			≈ 8.55 *ms*
Proposed RL-SMFA	$6T_H + 3T_{EM}$	$6T_H + 3T_{EM}$	$8T_H$	$20T_H + 6T_{EM} \approx 2.65$ *ms*

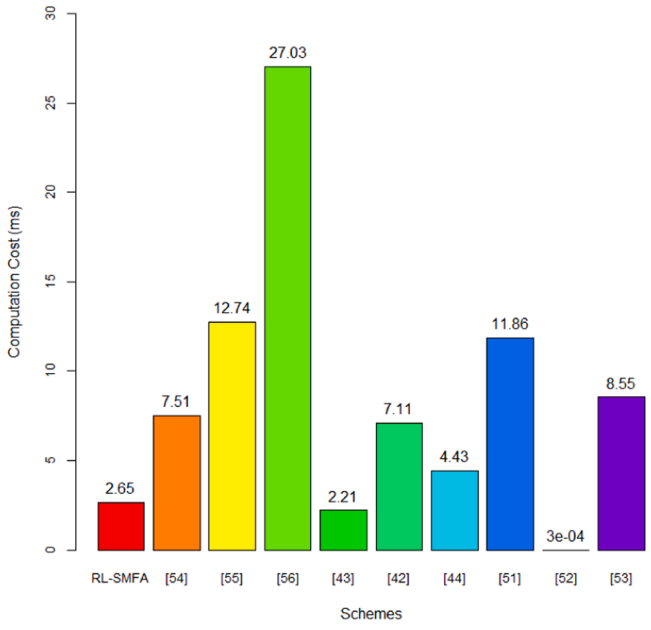

Fig. 6. Comparison of computation overhead (*ms*).

[41–43,50–55] to examine the cost of computing resources limited to memory utilization while analyzing the efficiency of key agreement mechanisms. In order to examine their cost factors, different computing parameters are considered such as public key over elliptic-curve cryptography $pk_{ecc} \approx 64$ *bits*, symmetric key s_k, random integers r_i, device/user identity $id \approx 16$ *bits*, long term shared key s_k, length of prime field *len*, order of an elliptic curve o_{ec}, hash algorithm $h_a \approx 32$ *bits*, timestamp $t_s \approx 4$ *bits*, ephemeris data $e_p \approx 40$ *bits*, and exponential operation $e_{op} \approx 128$ *bits* respectively. The bandwidth efficiencies of the proposed RL-SMFA and other existing schemes [41–43,50–55] are shown in Table 5 to examine the cost factors namely bw_{Int}, bw_{Aka}, bw_{Tot}, and bw_{Avg} involved during the authentication and key agreement phase. The proposed RL-SMFA composes of two authentic message requests as

Table 5
Bandwidth utilizations of the proposed RL-SMFA and other schemes.

Schemes	Message Requests	bw_{Int} (*bits*)	bw_{Aka} (*bits*)	bw_{Tot} (*bits*)
Ma et al. [53]	$\{k, q, P, \mathbb{G}, p_{pub}, h_i\}$, $\{AID_{ui}, T_{ui}, R_1, \alpha\}$, $\{AUD_{ui}, AID_{fnj}, T_{ui}, T_{fnj}, R_1, R_2, \alpha, \beta\}$, and $\{R_2, R_3, T_{CS}, \gamma\}$	248	352	600
Gope et al. [54]	$\{pid_{iu}, f_{id}\}$, $\{pid^*, N_s, C_i, Res_{Serv}\}$, and $\{R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{uav}, EL\}$	32	664	696
Ever [55]	$\{PID_{MS}, b_j, c_j, zN_j\}$, $\{m, \Delta_j, TS_S\}$, and $\{S_{k1}, PID_j, CH_{IDj}, TS_C\}$	160	208	368
Azrour et al. [42]	$\{V, \alpha, b, M_{ID}\}$, $\{V_1, M_I, D, A, ID_{SN}, T_1\}$, $\{V_2, B, M_I, D, T_2\}$, $\{V_3, C, H_I, D, ID_{SN}, T_3\}$, and $\{V_4, D, ID_{SN}, T_4\}$	128	528	656
Lwamo et al. [41]	$\{ID_{im}, ID_{ih}, RN_i, T_1\}$ and $\{RN_i, RN_s, R_c, A_i\}$	100	272	372
Bagga et al. [43]	$\{R_{eq1}, R_{eq2}, R_{eqi}, H_{id}, TS_1\}$, $\{R_{eq1}, R_{eq2}, R_{eqi}, HID_i, VHID_j, R_{eq3}, R_{eq4}, TS_2\}$, $\{R_{eq5}, R_{eq6}, R_{eqCS}, TS_3\}$, $\{R_{eq5}, H_{SK}, TS_4\}$	340	1216	1556
Koutsos [50]	$\{n_j, sqn_r, MAC_{km-id}\}$, $\{n_j, sqn_{id-n}, fk_{id}, MAC_{km-id}, GUTI_{n-id}\}$, and $\{id, guti_u, n_j\}$	200	432	632
Fan et al. [51]	$\{SUP_i, R, pk\}$, $\{rand, xres, ck, ik, autn, mac\}$, and $\{av, xmac, xautn, k_{ausf}, mk\}$	112	448	560
Cao et al. [52]	$\{ID_{SN}, T_x, K_{sn}, p, E_1, MAC_1\}$, $\{ENC_K, T_y, K_{sn}, p, K_{ue}, MAC_2\}$, and $\{MAC_3\}$	260	484	744
Proposed RL-SMFA	$\{ID_i, I_{gd}, H(.), \eta_i, \alpha_i, \beta_i, sk_i, PD_{sk}\}$ and $\{D_{ID}, \varepsilon_i, PD_K, PT_m\}$	248	152	400

$\{ID_i, I_{gd}, H(.), \eta_i, \alpha_i, \beta_i, sk_i, PD_{sk}\}$ and $\{D_{ID}, \varepsilon_i, PD_K, PT_m\}$ to find its computing efficiency $bw_{Int} \approx [16 + 16 + 32 + 40 + 40 + 40 + 32 + 32 = 248\ bits]$, $bw_{Aka} \approx [16 + 40 + 32 + 64 = 152\ bits]$, and $bw_{Tot} \approx [248 + 152 = 400\ bits]$.

Lwamo et al. [41] include two requested messages as $\{ID_{im}, ID_{ih}, RN_i, T_1\}$ and $\{RN_i, RN_s, R_c, A_i\}$ to determine $bw_{Int} \approx [16 + 16 + 64 + 4 = 100\ bits]$, $bw_{Aka} \approx [64 + 64 + 16 + 128 = 272\ bits]$, and $bw_{Tot} \approx [100 + 272 = 372\ bits]$. Azrour et al. [42] require five authentic messages such as $\{V, a, b, M_{ID}\}$, $\{V_1, M_I, D, A, ID_{SN}, T_1\}$, $\{V_2, B, M_I, D, T_2\}$, $\{V_3, C, H_I, D, ID_{SN}, T_3\}$, and $\{V_4, D, ID_{SN}, T_4\}$to gain the cost factors $bw_{Int} \approx [32 + 40 + 40 + 16 = 128\ bits]$, $bw_{Aka} \approx [32*4 + 40*6 + 64*2 + 16*1 + 4*4 = 528\ bits]$, and $bw_{Tot} \approx [128 + 528 = 656\ bits]$. Bagga et al. [43] use four message requests as $\{R_{eq1}, R_{eq2}, R_{eqi}, H_{id}, TS_1\}$, $\{R_{eq1}, R_{eq2}, R_{eqi}, HID_i, VHID_j, R_{eq3}, R_{eq4}, TS_2\}$, $\{R_{eq5}, R_{eq6}, R_{eqCS}, TS_3\}$, $\{R_{eq5}, H_{SK}, TS_4\}$ to acquire $bw_{Int} \approx [128*2 + 64 + 16 + 4 = 340\ bits]$, $bw_{Aka} \approx [128*9 + 16*3 + 4*4 = 1216\ bits]$, and $bw_{Tot} \approx [340 + 1216 = 1556\ bits]$. Ma et al. [53] execute five message requests such as $\{k, q, P, \mathbb{G}, p_{pub}, h_i\}$, $\{AID_{ui}, T_{ui}, R_1, \alpha\}$, $\{AUD_{ui}, AID_{fnj}, T_{ui}, T_{fnj}, R_1, R_2, \alpha, \beta\}$, and $\{R_2, R_3, T_{CS}, \gamma\}$ to obtain $bw_{Int} \approx [40*3 + 32*2 + 64 = 248\ bits]$, $bw_{Aka} \approx [16*6 + 32*3 + 40*4 = 352\ bits]$, and $bw_{Tot} \approx [248 + 352 = 600\ bits]$. Gope et al. [54] operate three message requests as $\{pid_{iu}, f_{id}\}$, $\{pid^*, N_s, C_i, Res_{Serv}\}$, and $\{R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{uav}, EL\}$ to secure $bw_{Int} \approx [16*2 = 32\ bits]$, $bw_{Aka} \approx [16*2 + 128*3 + 40*3 + 64*2 = 664\ bits]$, and $bw_{Tot} \approx [32 + 664 = 696\ bits]$.

Ever [55] exchanges three authentic messages such as $\{PID_{MS}, b_j, c_j, zN_j\}$, $\{m, \Delta_j, TS_S\}$, and $\{S_{k1}, PID_j, CH_{IDj}, TS_C\}$ to attain $bw_{Int} \approx [16 + 40*2 + 64 = 160\ bits]$, $bw_{Aka} \approx [128 + 16*2 + 40 + 4*2 = 208\ bits]$, and $bw_{Tot} \approx [160 + 208 = 368\ bits]$. Koutsos [50] shares three transmission requests as $\{n_j, sqn_r, MAC_{km-id}\}$, $\{n_j, sqn_{id-n}, fk_{id}, MAC_{km-id}, GUTI_{n-id}\}$, and $\{id, guti_u, n_j\}$ to achieve $bw_{Int} \approx [40 + 128 + 32 = 200\ bits]$, $bw_{Aka} \approx [40*2 + 128*2 + 32*3 = 432\ bits]$, and $bw_{Tot} \approx [200 + 432 = 632\ bits]$. Fan et al. [51] share three authentic requests as $\{SUP_i, R, pk\}$, $\{rand, xres, ck, ik, autn, mac\}$, and $\{av, xmac, xautn, k_{ausf}, mk\}$ to find $bw_{Int} \approx [16 + 32 + 64 = 112\ bits]$, $bw_{Aka} \approx [64*3 + 128*2 = 448\ bits]$, and $bw_{Tot} \approx [112 + 448 = 560\ bits]$. Cao et al. [52] generates $\{ID_{SN}, T_x, K_{sn}, p, E_1, MAC_1\}$, $\{ENC_K, T_y, K_{sn}, p, K_{ue}, MAC_2\}$, and $\{MAC_3\}$ to acquire $bw_{Int} \approx [32 \times 4 + 4 + 64 \times 2 = 260\ bits]$, $bw_{Aka} \approx [128*3 + 4 + 32*3 = 484\ bits]$, and $bw_{Tot} \approx [260 + 484 = 744\ bits]$. Table 5 shows the bandwidth utilization of the proposed RL-SMFA and the other schemes [41–43,50–55]. The distinctive results show that the proposed RL-SMFA consumes less communication overhead than related schemes [41,43,47–49] except for Lwamo et al. [41] and Ever [55]as shown in Fig. 7.

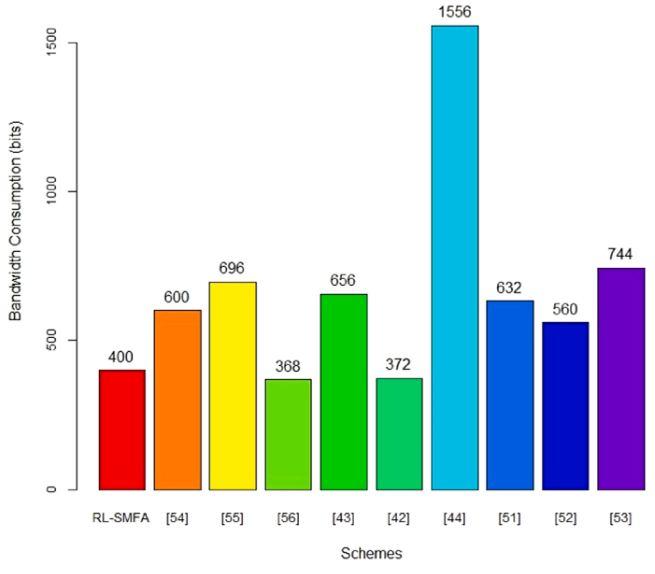

Fig. 7. Comparison of bandwidth utilization rate($bits$).

6.5. Analysis V: energy consumption

This analysis considers the battery-based operation of the drone system to compute the consumption of energy within the renewal of key agreement protocols driven by the drone controller. The device controller uses the proposed RL-SMFA and other existing schemes to measure their energy consumption using a one-time activation function per second. In order to analyze the consumption ratio, the modular design applies a dedicated flight controller i.e., DJI MATRICE M600 Pro [69] which has a battery capacity $\approx 4500\ mAh$ to operate smart device connectivity over 30 *minutes*. In this practical simulation, the timeline graph considers the measurement data of the energy consumption which analyze the beacon period to correlate the performance ratio of the proposed RL-SMFA and other existing schemes over the flight duration of the drone system. The operational scenario has the following steps:

Step 1 : Assign a root node as a mother drone that connects the ground control station directly to examine the device activities over a long distance.
Step 2 : Design a tree topology with drone connectivity via ground control station to initiate session key to the nearest drone and to establish secure communication.
Step 3 : Utilize the session key between the drone systems to examine the consumption ratio of the communication links.
Step 4 : Guarantee a constant speed with drone mobility model 5 m/s, 4 m/s, and 3 m/s to operate and monitor the drone operation via a dedicated channel i.e., WiFi.
Step 5 : Adopt mobility model with constant acceleration $\approx 4m/s^2$ to examine the signaling data over different data rates i.e., 1 *Mbps* and 2 *Mbps* acquired with a payload of ≈ 1024 *bytes*.
Step 6 : Implement the drone software on a Raspberry Pi Zero [W] [70] and configured the open-source operation system i.e., Ubuntu 20.04 to explore three major parts such as remote control relay, AT command, drone identification, and tracking.
Step 6.1 : Apply transport layer security protocol i.e., authentication and key agreement phase of the proposed RL-SMFA and other existing schemes to share the data transmission securely between the host terminal [Raspberry Pi Zero W] and hardware security module [HSM].
Step 6.2 : Exploit the command library like glibc 2.24 to host OPTIGA Trust X written in C language to initialize two threads such as reading and parsing the inputs generated by Bluetooth tools.
Step 6.3 : Execute cryptographic library to analyze the security features of the proposed RL-SMFA and other existing schemes to optimize the low power computing devices, especially in the B5G era.
Step 6.4 : Examine the storage limitation of the DJI MATRICE M600 Pro-using TCP/IP sockets to analyze the design structure of the flight control server application via packet switch, remote control, and drone identification.
Step 7 : Extract *main.py*, *main WIndow.py*, *and location.py* to separate the functional threads and to compute the energy models E_M using:

$$E_M = \frac{P}{V_\alpha},$$

where $P = \frac{(\sum_{k=1}^{3} m_k) g v_\alpha}{\mathfrak{M}} + P_l$, m_k is an operational headwind, v_α is a battery recharge efficiency, P_l is payload data, g is a unitless factor, and $\mathfrak{M}$ is a power multiplied by traveling time.

In the systematic analysis, a beacon period $\approx 200\ ms$ is set to address the complexities of the key agreement mechanisms which operate at $2.4GHz$ to examine the efficiency of the transmission mode. To fairly

compare the operational scenario, the drone systems are equipped with user datagram protocol (UDP) based on NAT strategy. The ground control station relies on a few assumptions including hash 1.23 *mAh* and encryption/decryption 2.66 *mAh* to allow communication with the drone systems via the mother drone. The examination result revealed that the proposed RL-SMFA consumed less computation power to process send/receive data packets as it has less parameter utilization during the login and authentication phase to maintain a better message delivery with less fluctuation/interruption than other existing schemes shown in Fig. 8.

6.6. Analysis VI: simulation environment

This analysis applied a tool of ns3 simulator to compare the key agreement phases of the proposed RL-SMFA and other existing schemes [71]. The performance of key agreement phases was measured using a converge-cast tree which uses a drone to generate the data packets and route it through the gateway node. The quality metrics such as end-to-end delay and packet delivery ratio were chosen to examine the performance of the computing environment via node scheduling. The computing environment utilized a geographical grid model with its size varied between 4×4 and 16×16 to examine the mobility ≈ 80 *meters*. In the grid environment, the drone was highly diversified between 30 and 180 to evaluate its computation results and initiated the computing services between the drones via a gateway to analyze the performance of the proposed RL-SMFA and other existing schemes.

This model initialized the energy of a drone node ≈ 2000 *Joule* and had a gateway with a dedicated mechanism to supply a fresh battery source when the drone node landed. The drone uses a few specific constraints like power propulsion to reserve enough energy and limit the usage of flight time without any additional radioactivity scheduling. The power consumption explored different computing states such as idle, sleep, transmit, and receive via Intel Pro-WiFi to activate the duty cycle $\approx$ *by* 10% with a transceiver period $\approx 1sec$. To manage the active duration $\approx 0.1sec$, the sleep period shortens the period of data transmission with a few additional specifications as shown in Table 6. The opportunistic network utilized a dedicated source node with a constant speed $\approx$ *of* 15 m/s flying at an attitude $\approx 20m$ to limit the flight duration 15 *minutes*.

In the scheduled time, the source node traveled $\approx$ 90% to perform data collection and $\approx$ 10% to schedule data gathering via a realistic scenario with random events. This node is scheduled to transmit the data packets 200 *nos* where each packet has 1500 *bytes* long. The generated data packet had an interval of $\approx 2sec$ to deliver it to an opportunistic network via source drone with a beacon message *'Hello'*. In case of unsuccessful transmission, the opportunistic network initiates a beacon message *'Hello'* via an authorized gateway to perform data gathering. The network simulated with a source drone to vary the packet transmission between 10% to 100% and sensed images/sound $\approx$ 300 *KB* randomly through the realistic scenario to the sink node. The realistic scenario was set with a random seed to execute the simulation $\approx$ 10 *times* to analyze the computation values.

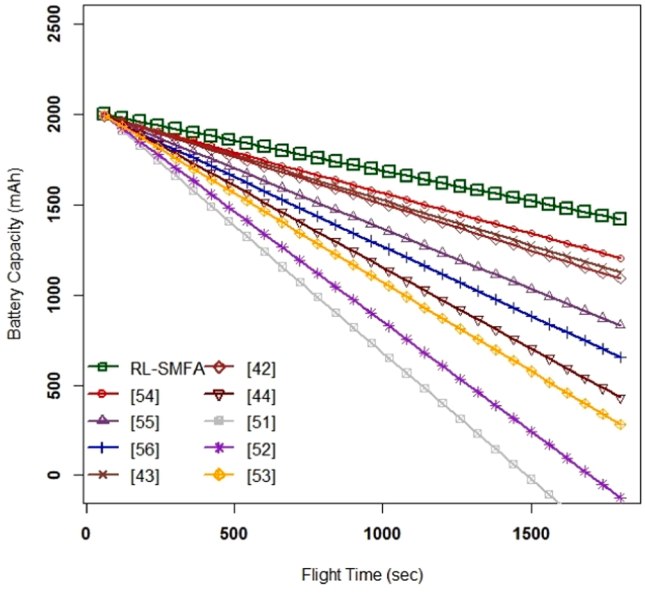

Fig. 8. Flight time versus battery capacity (*mAh*).

Table 6
Important parameters of wireless communication channel.

Network Parameter	Assigned Value
PHY / MAC Model	IEEE 802.11n [2.4 GHz]
Rate of Data Transmission	11 Mbps
Control Message	ACK/RTS/CTS
Propagation Loss Model	Free Space Propagation Model [FRIIS]
Signal Detection Threshold Using CSMA	− 96 *dBm*
Signal Energy Detection	− 86 *dBm*
Antenna Type	Omnidirectional
Antenna Gain	0 *dBi*
Geographical Grid Model	4×4 and 16×16
Mobility	$\approx$ 80 *meters*

The analysis utilized the sensing applications to perform sporadic communication and applied event-driven programming to handle the incoming signals via a converge-cast tree without any additional radio activity mechanism. The sensing drones varied between 30 and 180 with the probability of source node $\approx$ 50% to carry out the effectiveness of initial and final execution. The executed results explored the PHY/MAC model to evaluate the performance of the network which observes a few communication metrics such as throughput rate, packet delivery ratio, and end-to-end delay to maintain better data maintenance and connectivity in any surveillance network. The evaluation result considered the flow of transmission to analyze the effectiveness of data exchange between the drones adopted with a flight speed $\approx$ *of* 10 m/s.

Average Throughput Rate (ATR) measures the rate of data transmission at which the drone system revolves around the surveillance network to obtain the amount of information successfully received by the source drone. It is defined as

$$ATR = \frac{\sum_{k=i}^{N} Amount\ of\ Bytes\ Received\,(k) \Big/ \left(\begin{matrix} Last\ Received\ Packet\ Time(k) + \\ First\ Received\ Pcket\ Time\,(k) \end{matrix} \right)}{N} \tag{1}$$

Eq. (1) is composed of computing bytes obtained in the exchange of message transmission which considers the propagation delay of each data flow (k) ordered by the volume of network traffic (N). In the experimental scenario, the communication metric received the system logs of the MAC/PHY layer to sense the propagation parameters including path loss, transmitted, and received bytes $\approx 1ns$ to observe the performance of the network. This metric considered the number of drones to compute its constant bit rate (CBR) and utilized a network interface of 802.11n to investigate the channel frequency $20MHz$ to $40MHz$. The adopted simulation settings investigate the 802.11n interface to read the data packets of the drone using channel frequency. The drone utilized the simulation settings to establish its communication with neighbor one via a trusted gateway to probe the total volume of data traffic implicitly measured by its packet loss. The proposed RL-SMFA shares its system parameters proactively with the network interface whereby the channel quality index is improved to maintain a better throughput rate than other existing schemes [41–43,50–55] shown in Fig. 9.

Packet Delivery Ratio (PDR) relates to the delivery capacity of the network generated by drone-to-drone communication via a trusted gateway to observe the delivery ratio of the packets originating from the

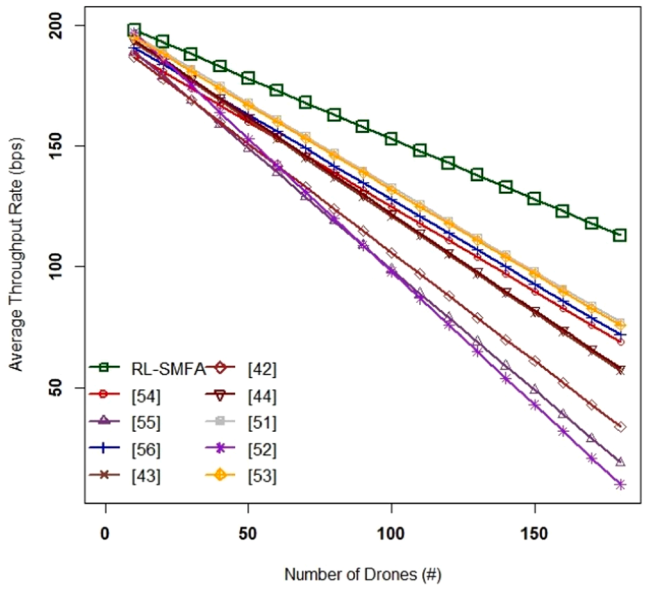

Fig. 9. Number of drones versus average throughput rate (*bps*).

source drone. In order to analyze the processing capacity of the network interface, the application layer observed the number of packets received by the CBR sink. The delivery ratio is defined as:

$$PDR = \frac{Total\ number\ of\ Received\ Packets}{(Total\ number\ of\ Received\ Packets + Total\ number\ of\ loss\ packets)} \quad (2)$$

In this case, the system parameters of the proposed RL-SMFA had better existence with intermediate waypoints via a trusted gateway to offer a reliable delivery rate that homogeneously maintains the effectiveness of device connectivity to improve the packet delivery ratio ≈ 78.5% of the network than other existing schemes [41–43,50–55] shown in Fig. 10.

End-To-End Delay (E2E-D) considers a few significant parameters such as packet length and link transmission rate to analyze the propagation delay typically ranging from $2 \times 10^8 m/s$ to $3 \times 10^8 m/s$. The network uses a dedicated interface to examine the functional performance of the store-and-forward system where the drone node finds its destination through a next-hop router to transmit and receive the generated packets successfully. This is mathematically computed as:

$$E2E - D = \sum_{k=1}^{N_P} \frac{(TRS_i - TSN_i)}{N_P} \quad (3)$$

where TRS_i and TSN_i are the valued time to send and receive the i^{th} packets successfully and N_P is the total number of generated packets. The access control and key establishment of the proposed RL-SMFA and other existing schemes utilize their message requests between the drone systems via a trusted gateway to investigate the average latency obtained by the received packets. To associate the connectivity with the applied settings, the proposed RL-SMFA and other existing schemes [41–43,50–55] extracted their system parameters using short headers. The analytical result shows that the proposed RL-SMFA obtains a higher transmission rate as it can efficiently manage the desirable features of mobility networks to achieve a high volume of transmitted bytes with less computation delay ≈ 0.253 *sec* than other existing schemes shown in Fig. 11.

7. Discussion on comparative results

The drone application has gained prominence for various military observations including surveillance, medical transport, aerial photography, and medical transport. The observation utilizes its planning strategy to analyze the physical characteristics of the collaborative drone network to optimize the conversion speed with different operation modes namely takeoff, searching, and tracking [72]. Each mode densely observes the processing and communication capabilities of terrestrial network devices to impart computing services through the ground station to remote users. The ground station uses the frequency of the wireless channel to send the control commands to the drone system and has a beneficiary of a remote user to access the real-time information controlled by the drones. As drone networks gain information retrieval using wireless channels, the exchange of information between remote users may address various security threats and vulnerabilities. In other words, drone networks employ next-generation networks to design a massive machine-type communication (mMTC) that focuses on the development of B5G to discover a security architecture standardized by a third-generation partnership project (3GPP) [73].

To offer a better computing service with cloud architecture, mMTC is integrated with various emerging application systems including

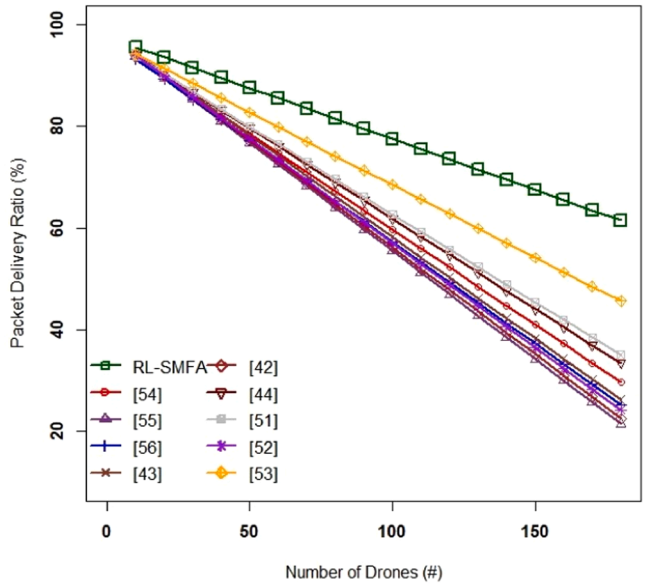

Fig. 10. Number of drones versus packet delivery ratio (%).

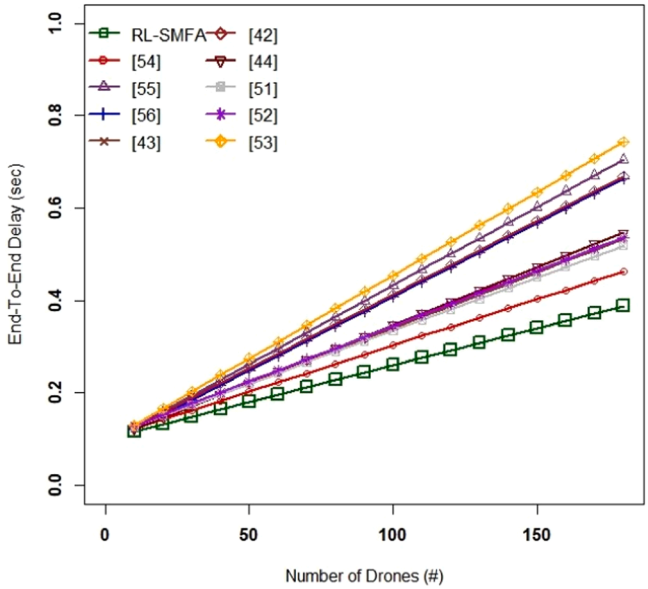

Fig. 11. Number of drones versus end-to-end delay (*sec*).

autonomous driving and logistics. However, recent studies revealed that native security architecture like 5 G AKA cannot prevent a few security vulnerabilities such as stolen devices, impersonation, and password guessing. Therefore, this paper presents robust lightweight secure multi-factor authentication which integrates a few additional security features to handle issues of 5 G AKA. The results obtained in Section 6 demonstrated the key significance of the proposed RL-SMFA and other existing schemes in terms of signaling, computation, communication, bandwidth, and energy consumption. The brief summary of the evaluation reports is as follows:

1 The comparison of signaling cost with the proposed RL-SMFA and other existing schemes [41–43,50–55] shows that the proposed RL-SMFA operates less signaling messages between the users via a trusted gateway to protect the network privacy and to retain the original merits of device registration and access control.
2 The distinguished result of computation cost signifies that the proposed RL-SMFA employs lightweight operation to influence the authenticity of the message transmission between the users via a trusted gateway. Moreover, the trusted gateway distinctively chooses the identities of all the deployed drones to share their unique secret key with the remote users in order to extract the user credentials.
3 The contrariety of communication costs with the proposed RL-SMFA and other existing schemes [41–43,50–55] reveals that the proposed RL-SMFA ensures better message security and conditional privacy during the authentication process to solve unreliable signal connection in the use of B5G communications.
4 The distinctive result of bandwidth utilization with the proposed RL-SMFA and other existing schemes [41–43,50–55] exhibits that the proposed RL-SMFA offers seamless network access through its parameter utilization to perform symmetric operations including encryption and decryption. Moreover, a core network like B5G can use adaptive resource utilization to minimize the consumption rate of bandwidth and optimize resource scheduling via a trusted gateway in order to satisfy the criteria of quality of service (QoS).
5 The hardware assessment using DJI MATRICE M600 Pro-demonstrates that the proposed RL-SMFA utilizes fewer computation operators to generate the message requests using an authentication mechanism and establishes secure communication between the remote users via a trusted gateway to optimize the rate of energy consumption. Further, the trusted gateway shares the session key with the registered drone to guarantee traceability and accountability of the communication requests.
6 The simulation analysis using ns3 discloses that the proposed RL-SMFA utilizes a trusted gateway to collect or share the generated data between the remote users which solve the issue of inadequate network coverage in the surveillance area [60]. Moreover, the proposed RL-SMFA uses minimum transmission rounds during the authentication phase to improve a few quality metrics including throughput rate, packet delivery ratio, and end-to-end delay.

The above analysis shows that the proposed RL-SMFA is more secure and utilizes fewer computation operators to generate a valid authentic request between the users via a trusted gateway whereby the cost efficiencies are considerably reduced than other existing schemes [41–43, 50–55] in most cases. However, the proposed scheme has some limitations to address in the future to support unlinkability and group-based authentication. Also, in the proposed RL-SMFA, a key property like session unlinkability is not considered fully as the privacy and availability of the users are mutually traded off to resist denial of service attack.

8. Conclusion

Smart surveillance and device mobility utilizes aerial vehicles to exchange sensitive information between civilians and drones. It may use interconnected components to construct an intelligent drone that enhances people's safety and ensures quality of service. Because information sharing is highly sensitive and open to communication media, flying zones demand a multi-factor authentication framework to preserve device security and privacy. Of late, small-scale UAVs have been employed in a host of systems, including package delivery, disaster management, and geographic mapping. In order to verify security features of flying zones, several authentication schemes have been proposed. However, the existing schemes do not explore authentication strategies like unique secret keys and validated requests to strengthen security efficiencies in military applications. Therefore, to address the security issues effectively, this paper proposed robust lightweight multi-factor authentication that uses a fast hash function to perform system verification that resolves the time synchronization problem. Formal and informal security proofs showed that the proposed RL-SMFA can fulfill all the demands of military health systems better than other authentication schemes. Performance analysis showed that the proposed RL-SMFA has less cost efficiency including computation, communication, bandwidth, and energy to enhance the performance efficiency of surveillance systems. Finally, the simulation study using ns3 demonstrated the effectiveness of link establishment using authentication mechanisms including proposed RL-SMFA and the existing schemes to signify the impact of quality metrics such as throughput rate, packet delivery ratio, and end-to-end delay.

In the future, the proposed RL-SMFA will incorporate a technical strategy of mutual handshakes to validate the complexity of the authentication framework, using a suitable cryptographic algorithm to estimate the execution cost of surveillance networks. Also, a practical testbed will be designed to analyze the functional features of the IoT devices and apply wireless communication protocols to ensure sufficient network coverage and deployment cost to broadcast sensitive information in a remote zone.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported by the National Research Foundation of Korea funded by the MSIT (Ministry of Science, ICT) under Grant 2022H1D3A2A02081848 and by the Gachon University research fund under Grant GCU-202206210001.

References

[1] N.H. Motlagh, T. Taleb, O. Arouk, Low-altitude unmanned aerial vehicles-based internet of things services: comprehensive survey and future perspectives, IEEE Internet Things J. 3 (6) (2016) 899–922.
[2] M. Mozaffari, W. Saad, M. Bennis, Y.H. Nam, M. Debbah, A tutorial on UAVs for wireless networks: applications, challenges, and open problems, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2334–2360.
[3] M.R. Yuce, Implementation of wireless body area networks for healthcare systems, Sens. Actuators A 162 (1) (2010) 116–129.
[4] I. Lee, K. Lee, The Internet of Things (IoT): applications, investments, and challenges for enterprises, Bus. Horiz. 58 (4) (2015) 431–440.
[5] Z. Wang, Z. Yang, T. Dong, A review of wearable technologies for elderly care that can accurately track indoor position, recognize physical activities and monitor vital signs in real time, Sensors 17 (2) (2017) 341.

[6] P. de Moerloose, K. Fischer, T. Lambert, J. Windyga, A. Bátorová, G. Lavigne-Lissalde, C. Hermans, Recommendations for assessment, monitoring and follow-up of patients with haemophilia, Haemophilia 18 (3) (2012) 319–325.
[7] B.D. Deebak, F. Al-Turjman, M. Aloqaily, O. Alfandi, An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT, IEEE Access 7 (2019) 135632–135649.
[8] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, L. He, A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems, J. Med. Syst. 38 (1) (2014) 9994.
[9] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.K.R. Choo, P. Burnap, Impact and key challenges of insider threats on organizations and critical businesses, Electronics 9 (9) (2020) 1460.
[10] P. Krishnamurthy, J. Kabara, T. Anusas-Amornkul, Security in wireless residential networks, IEEE Trans. Consum. Electron. 48 (1) (2002) 157–166.
[11] Y. Ren, L. Zhang, P.N. Suganthan, Ensemble classification and regression-recent developments, applications and future directions, IEEE Comput. Intell. Mag. 11 (1) (2016) 41–53.
[12] X. Liu, C. Qian, W.G. Hatcher, H. Xu, W. Liao, W. Yu, Secure internet of things (iot)-based smart-world critical infrastructures: survey, case study and research opportunities, IEEE Access 7 (2019) 79523–79544.
[13] N.H. Abd Rahim, S. Hamid, M.L.M. Kiah, S. Shamshirband, S. Furnell, A systematic review of approaches to assessing cybersecurity awareness, Kybernetes 44 (4) (2015) 606–622.
[14] S.H. Islam, G. Biswas, Dynamic ID-based remote user mutual authentication scheme with smartcard using elliptic curve cryptography, J. Electron. 31 (2014) 473–488. China.
[15] M. Sarvabhatla, C.S. Vorugunti, A secure and robust dynamic ID-based mutual authentication scheme with smart card using elliptic curve cryptography, in: Proceedings of the Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), Bengaluru, India, 2015, 14–18 September.
[16] S. Kalra, S.K. Sood, Secure authentication scheme for IoT and cloud servers, Pervasive Mob. Comput. 24 (2015) 210–223.
[17] S. Kumari, M. Karuppiah, A.K. Das, X. Li, F. Wu, N. Kumar, A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers, J. Supercomput. 74 (2017) 6428–6453.
[18] C.C. Chang, H.L. Wu, C.Y. Sun, Notes on "Secure authentication scheme for IoT and cloud servers, Pervasive Mob. Comput. 38 (2017) 275–278.
[19] J. Mo, Z. Hu, H. Chen, W. Shen, An efficient and provably secure anonymous user authentication and key Agreement for mobile cloud computing, Wirel. Commun. Mob. Comput. 2019 (2019), 4520685.
[20] K. Fan, Q. Luo, K. Zhang, Y. Yang, Cloud-based lightweight secure RFID mutual authentication protocol in IoT, Inf. Sci. 527 (2020) 329–340.
[21] B.D. Deebak, F. Al-Turjman, Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things, IEEE J. Sel. Areas Commun. 39 (2) (2020) 346–360.
[22] M. Hassanalian, A. Abdelkefi, Classifications, applications, and design challenges of drones: a review, Prog. Aerosp. Sci. 91 (2017) 99–131. May.
[23] M. Gharibi, R. Boutaba, S.L. Waslander, Internet of drones, IEEE Access 4 (2016) 1148–1162.
[24] R.J. Hall, An internet of drones, IEEE Internet Comput. 20 (3) (2016) 68–73. May/Jun.
[25] J. Won, S.H. Seo, E. Bertino, Certificateless cryptographic protocols for efficient drone-based smart city applications, IEEE Access 5 (2017) 3721–3749.
[26] B.D. Deebak, A.T. Fadi, Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing, Future Gen. Comput. Syst. 116 (2021) 406–425.
[27] A.T. Fadi, B.D. Deebak, Seamless authentication: for IoT-big data technologies in smart industrial application systems, IEEE Trans. Ind. Inf. 17 (4) (2020) 2919–2927.
[28] M.F. Ayub, K. Mahmood, S. Kumari, A.K. Sangaiah, Lightweight authentication protocol for e-health clouds in IoT based applications through 5G technology, Digit. Commun. Netw. 7 (2) (2020) 235–244.
[29] M.A. Kiran, S.K. Pasupuleti, R. Eswari, A lightweight two-factor mutual authentication scheme for cloud-based IoT, in: Proceedings of the 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), IEEE, 2019, pp. 1–6.
[30] M.K. Rao, S.G. Santhi, M.A. Hussain, Multi factor user authentication mechanism using internet of things, in: Proceedings of the Third International Conference on Advanced Informatics for Computing Research, 2019, pp. 1–5.
[31] L. Loffi, C.M. Westphall, L.D. Grüdtner, C.B. Westphall, Mutual authentication with multi-factor in IoT-Fog-Cloud environment, J. Netw. Comput. Appl. 176 (2021), 102932.
[32] B.D. Deebak, F. Al-Turjman, A smart lightweight privacy preservation scheme for IoT-based UAV communication systems, Comput. Commun. 162 (2020) 102–117.
[33] J.J. Jena, S.C. Satapathy, Use of evolutionary algorithms for detection of fatal diseases via DNA micro-array classification: a review, Commun. Softw. Netw. 134 (2021) 649–656.
[34] A.K. Sahoo, S.K. Mishra, B. Majhi, G. Panda, S.C. Satapathy, Real-time identification of fuzzy PID-controlled maglev system using TLBO-based functional link artificial neural network, Arab. J. Sci. Eng. 46 (2021) 1–16.
[35] P. Gope, A.K. Das, Robust anonymous mutual authentication scheme for n-times ubiquitous mobile cloud computing services, IEEE Internet Things J. 4 (5) (2017) 1764–1772.
[36] S. Dey, Q. Ye, S. Sampalli, Amlt: a mutual authentication scheme for mobile cloud computing, in: Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 700–705.
[37] B.B. Gupta, M. Quamara, An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards, Procedia Comput. Sci. 132 (2018) 189–197.
[38] G. Sharma, S. Kalra, A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications, J. Inf. Secur. Appl. 42 (2018) 95–106.
[39] F. Wang, Y. Xu, L. Zhu, X. Du, M. Guizani, LAMANCO: a lightweight anonymous mutual authentication scheme for $ N $-times computing offloading in IoT, IEEE Internet Things J. 6 (3) (2018) 4462–4471.
[40] L. Zhou, X. Li, K.H. Yeh, C. Su, W. Chiu, Lightweight IoT-based authentication scheme in cloud computing circumstance, Future Gen. Comput. Syst. 91 (2019) 244–251.
[41] N.M. Lwamo, L. Zhu, C. Xu, K. Sharif, X. Liu, C. Zhang, SUAA: a secure user authentication scheme with anonymity for the single & multi-server environments, Inf. Sci. 477 (2019) 369–385.
[42] M. Azrour, J. Mabrouki, R. Chaganti, New efficient and secured authentication protocol for remote healthcare systems in cloud-iot, Secur. Commun. Netw. 2021 (2021) 1-12.
[43] P. Bagga, A. Mitra, A.K. Das, P. Vijayakumar, Y. Park, M. Karuppiah, Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system, Comput. Commun. 195 (2022) 27–39.
[44] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, L. Liu, Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks, IEEE Trans. Netw. Sci. Eng. 8 (4) (2020) 2982–2994.
[45] Y. Xiao, S. Gao, 5GAKA-LCCO: a secure 5G authentication and key agreement protocol with less communication and computation overhead, Information 13 (5) (2022) 257.
[46] Y. Liu, L. Huo, G. Zhou, TR-AKA: a two-phased, registered authentication and key agreement protocol for 5G mobile networks, IET Inf. Secur. 16 (3) (2022) 193–207.
[47] A. Braeken, Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability, Comput. Netw. 181 (2020), 107424.
[48] A.K. Yadav, M. Misra, P.K. Pandey, A. Braeken, M. Liyange, An improved and provably secure symmetric-key based 5G-AKA Protocol, Comput. Netw. 218 (2022), 109400.
[49] J. Munilla, M. Burmester, R. Barco, An enhanced symmetric-key based 5G-AKA protocol, Comput. Netw. 198 (2021), 108373.
[50] A. Koutsos, The 5G-AKA authentication protocol privacy, in: Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2019, pp. 464–479.
[51] J. Fan, Y. Yan, Y. Kaiguo, Z. Lujing, Security analysis of 5G authentication and key agreement protocol, J. Tsinghua Univ. (Sci. Technol.) 61 (11) (2021) 1260–1266.
[52] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, H. Li, LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks, IEEE Internet Things J. 7 (6) (2020) 5329–5344.
[53] M. Ma, D. He, H. Wang, N. Kumar, K.K.R. Choo, An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks, IEEE Internet Things J. 6 (5) (2019) 8065–8075.
[54] P. Gope, B. Sikdar, An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones,, IEEE Trans. Veh. Technol. 69 (11) (2020) 13621–13630.
[55] Y.K. Ever, A secure authentication scheme framework for mobile-sinks used in the internet of drones applications, Comput. Commun. 155 (2020) 143–149.
[56] G. Lykou, D. Moustakas, D. Gritzalis, Defending airports from UAS: a survey on cyber-attacks and counter-drone sensing technologies, Sensors 20 (12) (2020) 3537.
[57] F. Firouzi, B. Farahani, M. Weinberger, G. DePace, F.S. Aliee, IoT fundamentals: definitions, architectures, challenges, and promises. Intelligent Internet of Things: From Device to Fog and Cloud, Springer, Cham, 2020, pp. 3–50.
[58] C. Pu, A. Wall, K.K.R. Choo, I. Ahmed, S. Lim, A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment, IEEE Internet Things J. 9 (12) (2022) 9918–9933.
[59] S. Hussain, S.A. Chaudhry, O.A. Alomari, M.H. Alsharif, M.K. Khan, N. Kumar, Amassing the security: an ECC-based authentication scheme for Internet of drones, IEEE Syst. J. 15 (3) (2021) 4431–4438.
[60] B.D. Deebak, F.H. Memon, S.A. Khowaja, K. Dev, W. Wang, N.M.F. Qureshi, C. Su, Lightweight blockchain based remote mutual authentication for AI-empowered IoT sustainable computing systems, IEEE Internet Things J. (2022), https://doi.org/10.1109/JIOT.2022.3152546.
[61] A. Kumar, H. Om, Handover authentication scheme for device-to-device outband communication in 5G-WLAN next generation heterogeneous networks, Arab. J. Sci. Eng. 43 (2018) 7961–7977.
[62] M. Rocchetto, N.O. Tippenhauer, CPDY: extending the Dolev-Yao attacker with physical-layer interactions, in: Proceedings of the Formal Methods and Software Engineering: 18th International Conference on Formal Engineering Methods, ICFEM 2016, Springer International Publishing, Tokyo, Japan, 2016, pp. 175–192. November 14-18, 2016, Proceedings 18.
[63] M. Fareed, A.A. Yassin, A lightweight and secure multilayer authentication scheme for wireless body area networks in healthcare system, Int. J. Electr. Comput. Eng. 13 (2) (2023) 1782.
[64] J. Lee, S. Yu, M. Kim, Y. Park, A.K. Das, On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks, IEEE Access 8 (2020) 107046–107062.

[65] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, H. Chen, Resource allocation and trust computing for blockchain-enabled edge computing system, Comput. Secur. 105 (2021), 102249.
[66] Z. Lv, The security of Internet of drones, Comput. Commun. 148 (2019) 208–214.
[67] D. Koo, Y. Shin, J. Yun, J. Hur, Improving security and reliability in Merkle tree-based online data authentication with leakage resilience, Appl. Sci. 8 (12) (2018) 2532.
[68] Miracl Cryptographic Sdk, 2019. https://github.com/miracl/MIRACL/. accessed 29 Nov,.
[69] L. Bertizzolo, M. Polese, L. Bonati, A. Gosain, M. Zorzi, T. Melodia, October). mmBAC: location-aided mmWave backhaul management for UAV-based aerial cells, in: Proceedings of the 3rd ACM Workshop on Millimeter-wave Networks and Sensing Systems, 2019, pp. 7–12.
[70] D.B.C. Lima, R.M.B. da Silva Lima, D. de Farias Medeiros, R.I.S. Pereira, C.P. de Souza, O. Baiocchi, A performance evaluation of raspberry Pi zero W based gateway running MQTT broker for IoT, in: Proceedings of the IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, 2019, pp. 0076–0081.
[71] M. Zia, M.S. Obaidat, K. Mahmood, S. Shamshad, M.A. Saleem, S.A. Chaudhry, A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system, IEEE Trans. Ind. Inf. 19 (2) (2022) 1683–1690.
[72] Y. Tang, Y. Miao, A. Barnawi, B. Alzahrani, R. Alotaibi, K. Hwang, A joint global and local path planning optimization for UAV task scheduling towards crowd air monitoring, Comput. Netw. 193 (2021), 107913.
[73] M. Wang, Z. Yan, A survey on security in D2D communications, Mob. Netw. Appl. 22 (2017) 195–208.

B D Deebak is presently working as Brain Pool Fellow in the department of computer engineering, at Gachon University, South Korea. He has more than 13 Years of Teaching and Research in various Engineering Institutions in India and Abroad. He received his Ph.D. under a research grant of TCS from SASTRA University-Thanjavur in 2016. His areas of research include Multimedia Networks, Network Security and Machine Learning. He is an active member in professional societies like IE (I), CSI and ISTE. His current research interests include network security, computer networks, wireless communication systems, wireless sensor networks, Multimedia Networks, Routing and Security. He has published 45 articles in well-reputed publishers such as IEEE, Elsevier, Springer and Tubitak. He also serves as reviewer from Elsevier-FGCS, IEEE Communications Letters, IEEE Access, IEEE Systems, and IEEE Sensors Journal.

Seong Oun Hwang received his BS degree in Mathematics in 1993 from Seoul National University, his MS degree in Information and Communications Engineering in 1998 from Pohang University of Science and Technology, and his Ph.D. degree in Computer Science from Korea Advanced Institute of Science and Technology. He worked as a software engineer at LG-CNS Systems, Inc. from 1994 to 1996. He worked as a senior researcher at Electronics and Telecommunications Research Institute (ETRI) from 1998 to 2007. He worked as a professor with the Department of Software and Communications Engineering at Hongik University from 2008 to 2019. He is currently a professor of the Department of Computer Engineering at Gachon University and an editor of ETRI Journal. His research interests include cryptography, cyber security, and artificial intelligence.