MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones

Zaid Ameen Abduljabbar[1,2], Vincent Omollo Nyangaresi[3], Junchao Ma[4(✉)], Mustafa A. Al Sibahee[4,5], Mustafa S. Khalefa[1], and Dhafer G. Honi[1]

[1] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
{zaid.ameen,mustafa.khalefa,dhafer.honi}@uobasrah.edu.iq
[2] Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen 518118, China
[3] Faculty of Biological and Physical Sciences, Tom Mboya University, Homabay 40300, Kenya
vnyangaresi@tmuc.ac.ke
[4] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
{majunchao,mustafa}@sztu.edu.cn
[5] Computer Technology Engineering Department, Iraq University College, Basrah, Iraq
mustafa.alsibahee@iuc.edu.iq

Abstract. Unmanned aerial vehicles have been deployed for surveillance in highly sensitive domains such as in the military. As such, the data exchanged between the operators and these aerial vehicles must be protected as any malicious access may lead to leakages and adversarial control of the drones. To achieve this, many schemes have been developed based on techniques such as blockchains, elliptic curve cryptography, dynamic keys, physically unclonable function, asymmetric and symmetric cryptography among others. However, majority of these protocols have been shown to be inefficient for deployment in this environment, while others have security holes that be exploited by attackers to cause mayhem in these networks. In this paper, a protocol that leverages on quadratic residues and Chinese remainder theorem is developed. Its security analysis shows that it offers mutual authentication, non-repudiation, unlinkability, identity privacy and traceability for misbehaving drones. It is also resilient against impersonation, forgery and replay attacks. In terms of performance, this protocol has the least execution time and relatively lower bandwidth requirements.

Keywords: Authentication · Drones · Encryption · MAC · Protocol · Privacy · Symmetric · UAV

1 Introduction

Unmanned Aerial Vehicles (UAVs) consist of airborne sensors and drones that communicate through wireless channels [1]. They are normally managed via radio remote control techniques and some inbuilt program control devices [2]. Due to their wider coverage, UAVs have been applied in a wide range of domains such as in the military,

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2022, LNICST 445, pp. 16–36, 2022.
https://doi.org/10.1007/978-3-031-15101-9_2

disaster monitoring, geological investigation, intelligence reconnaissance, aerial photography, television shooting and agricultural surveillance. In addition, they have been deployed to monitor roads and forests to prevent theft and forest fires. Moreover, they have facilitated the acquisition of detailed aerial images as well as the creation of detailed 3D models [3].

Despite the potential merits that UAVs present, security and privacy are major issues that need to be addressed. As explained in [4] and [5], UAVs lack communication security, and hence the need to develop protocols to secure the communication between the users and the drones. As explained in [2], attackers can forge, monitor, tamper or delete the packets being exchanged in UAV networks. In addition, authors in [6] identify Man-In-The-Middle (MITM), forgery and replay attacks as being serious issues in UAVs. Similarly, spoofing, Denial of Service (DoS), MITM and Telnet or File Transfer Protocol (FTP) attacks have been highlighted in [7] and [8] as being detrimental for UAV deployments. The reliance on open wireless channels for UAV communication has been identified in [9] and [10] as being the source of vulnerabilities and active attacks such as cloning, eavesdropping, physical capture, replays, MITM and node tampering. Further, the sensitive data in UAV devices or being exchanged over the open wireless channels need to be protected as any malicious capture, may lead to its compromise that may disrupt or interfere with normal operations [11].

Authors in [12] explain that the widespread usage of UAVs render security and computing resource utilization efficiency very crucial. Unfortunately, drones deployed in this environment are designed devoid of inbuilt security mechanisms [13, 14]. As such, privacy and security are thorny issues that require urgent solution [12, 15, 16]. As explained in [17], privacy is a major concern in UAVs owing to the sensitive data that is conveyed in these networks. One possible solution to these security challenges is strong identity authentication that must be executed before drones could commence packet exchanges [6]. In UAV networks, there is high mobility and hence the connection states keep on changing in terms of the links or serving base stations. As such, frequent authentications are required for these dynamic networks to prevent adversaries from accessing the network resources or causing any havoc [18].

In line with this, many security protocols have been developed over the recent past. However, majority of these protocols are not sufficient to curb typical UAV attacks [15]. Consequently, how to effectively protect UAVs from disruptions or unauthorized access is still an open challenge. Another setback related to security and privacy is the resource-constrained nature of the UAV sensors, which limit their computing power. As such, the sophisticated and frequent authentications may be detrimental to these devices [12]. There is therefore need to improve on operational efficiency of the UAV sensors through the deployment of lightweight security protocols [19]. The specific contributions of this paper include the following:

- A protocol that leverages on quadratic residues and Chinese remainder theorem is developed for secure traffic forwarding in UAVs.
- Message authentication codes are deployed to encipher the exchanged messages for enhanced integrity and privacy protection.
- Extensive formal and informal security analysis is carried out to show that our protocol offers mutual authentication and resilience against typical UAV attacks.

- Performance evaluation is executed to demonstrate that the proposed protocol exhibits lower bandwidth requirements and the least execution time.

The rest of this article is organized as follows: Sect. 2 presents related literature while Sect. 3 outlines the system mode. On the other hand, Sect. 4 presents the security analysis, while Sect. 5 details performance evaluation of the proposed protocol. Finally, Sect. 6 concludes the paper and gives future research directions.

2 Related Work

The ever-increasing UAV deployments and security challenges in these networks has seen the development of numerous techniques to address these issues. However, some of these protocols still have issues regarding their efficiency or susceptibility to attacks. For example, authors in [20] have introduced an authentication protocol for security enhancement. However, this scheme cannot offer sufficient privacy [21]. Similarly, the authentication protocol presented in [7] cannot provide physical security. On the other hand, the lightweight user authentication scheme in [22] fails to uphold forward key secrecy [12]. Based on temporal credentials, an anonymous authentication protocol is developed in [11]. However, it is vulnerable to traceability, impersonation and stolen verifier attacks. In addition, it has scalability issues and cannot provide anonymity [16, 23]. Moreover, although the protocols in [11] and [22] offer increased security levels, the deployment of bilinear pairing operations increase their computational complexities [10, 24]. On its part, the protocol in [23] is susceptible to de-synchronization attacks and cannot offer backward security [12]. Similarly, the protocol introduced in [25] has high communication costs, is susceptible to traceability attacks and cannot offer backward and forward key secrecy.

An anonymous lightweight authentication protocol is presented in [26] that is shown to resists many attacks, while a watermark based authentication technique is developed in [27]. Unfortunately, the scheme in [27] has high storage and computational complexities. Based on public and private keys, a Certification Authority (CA) based authentication mechanism is presented in [28]. However, this approach has high computation overheads and its reliance on CA may present a single point of failure [29]. Based on Physical Unclonable Function (PUF), a mutual authentication scheme is introduced in [30]. Unfortunately, this protocol fails to provide forward key secrecy [12]. Similarly, anonymous mutual authentication scheme is presented in [31] that is demonstrated to offer anonymity. However, the usage of Trusted Platform Modules (TPMs) render this protocol expensive. In addition, this scheme cannot resist node tampering as well as physical attacks [10]. Authors in [32] introduce a spanning tree-based protocol. Unfortunately, this scheme lacks some security features, which authors in [33] addressed. On the other hand, the lightweight protocol developed in [34] has diminished performance [4].

Using Public-Key Cryptosystem (PKC), authors in [35] present a privacy preserving protocol. However, the deployment of PKC can potentially lead to high computation complexity [36]. Although the scheme presented in [37] can resist node cloning attacks, it is only ideal in situations where error data appear more often [2]. On the other hand, the lightweight authentication scheme in [38] is robust against numerous attacks, but has high communication overheads. Similarly, the authentication protocol in [39] exhibits high performance due to its lightweight cryptographic operations, but has numerous security issues. On the other hand, the tag-based scheme in [40] potentially prevents tag compromise attacks. However, the tag is required to execute computationally expensive cryptographic operations which render it unsuitable for resource constrained tags [41]. Similarly, Elliptic Curve Cryptography (ECC) based user authentication technique presented in [42] has high communication and computation overheads. On the other hand, the authentication protocol introduced in [43] is susceptible to MITM, replay, password guessing, privileged insider attacks and cannot uphold forward security. Although the Software Define Networking (SDN) based protocol in [44] offers mutual authentication in multi-drone networks, it is vulnerable to session key violation attacks [12]. Using cryptographic identities, an authentication scheme is presented in [45] to offer privacy and device anonymity. However, this protocol cannot offer strong mutual authentication.

In order to provide privacy and security enhancements, a blockchain based protocol is developed in [46]. Unfortunately, the deployed blockchains results in high computation and storage costs [47]. Similarly, the exponential time complexities for the scheme in [48] makes it unsuitable for UAV sensors. Although the schemes in [49] and [50] offer some levels of physical security using PUFs, these protocols are unsuitable for large scale dynamic UAV networks. On the other hand, the two-way authentication protocol presented in [51] is susceptible to session key leakage, secret temporary parameter leakage, server and user emulation attacks [52]. In addition, it has scalability issues and cannot guarantee user anonymity. Based on noisy PUF, authors in [21] have introduced an authentication scheme, but the tag here is required to execute computationally expensive operations and store helper data which makes it unsuitable for UAV environment. Similarly, the authentication technique in [53] has expensive computation and communication overheads due to pairing operations [54].

Based on certificate based digital signatures, authors in [55] develop an authentication scheme, but which cannot provide protection against physical and location threats. Similarly, the user authentication scheme in [56] is insecure due to its susceptibility to numerous attacks [57]. On the other hand, the scheme in [58] is prone to impersonation and DoS attacks. Although the protocol in [59] offers forward security, it is still susceptible to offline password guessing and smart card loss attacks [60]. On the other hand, based on asymmetric key cryptography, authors in [61] have developed an authentication scheme for UAV sensors. However, asymmetric encryption has expensive computations [62] and hence this protocol is not ideal for this application. Authors in [63] present a pairing-free protocol, but which has issues with malevolent drone revocation. On the other hand, the protocol in [64] is vulnerable to de-synchronization and MITM attacks, and cannot uphold backward key secrecy. Similarly, although the scheme in [65] provides anonymity, it is vulnerable to replay, dictionary and privileged insider attacks.

Based on the discussions above, it is evident that most of the current schemes still have security issues, while others have performance challenges. For instance, in most of the PUF based protocols, there is need for exhaustive search operations during device identification. This results in high computation and storage costs, which is not ideal for large scale UAV environments. Similarly, blockchain, asymmetric key and PKC based protocols have high performance costs. The aim of this article is to address these issues by developing a lightweight symmetric key based authentication scheme that is not only secure but also has lower computation and communication overheads.

3 System Model

This section presents the mathematical preliminaries of the cryptographic primitives deployed in this paper. This is followed by the detailing of the procedures executed in the proposed protocol, as discussed in the following sub-sections.

3.1 Mathematical Preliminaries

The proposed protocol is based on some features of the Quadratic Residues (QRs) and Chinese Remainder Theorem (CRT). Here, we let m and s be any integer and natural numbers respectively. On condition that the greatest common divisor (G) of these numbers is unity, then m is a Quadratic Residue Modulo (QRM) s if the congruence q^2 can be solved in polynomial time. Mathematically, this G and congruence are expressed as in (1):

$$\mathrm{G(m,\ s)\ =\ 1;\ q^2\ =\ m\ (mod\ s)} \tag{1}$$

The solutions to the above expression are the modular square root of m (mod s). Suppose that e is an odd prime number such that G(m, e) = 1. In this case, m becomes a QRM of e if and only if (2) holds.

$$m^{\frac{e-1}{2}} = 1(\mathrm{mod\ e}) \tag{2}$$

On condition that m is QRM of e and $e = 3$ (mod 4), then the square roots of QR m modulo e is obtained as in (3).

$$\mathrm{R_{1,2}} = \pm m^{\frac{e+1}{4}} (\mathrm{mod\ e}) \tag{3}$$

Suppose that e and f are some two distinct odd prime numbers such that e = f = 3 (mod 4). If we let s = e.f and G(m, s) = 1, then m is a QRM s if and only if the conditions in (4) hold:

$$m^{\frac{e-1}{2}} = 1(\mathrm{mod\ e})\ \mathrm{and}\ m^{\frac{f-1}{2}} = 1\ (\mathrm{mod\ f}) \tag{4}$$

Based on (3), (4) and CRT, four modular square roots $\mathrm{R_{1,2,3,4}}$ of a QR m modulo s are derived as in (5).

$$\mathrm{R_{1,2,3,4}} = \pm \mathrm{j.f.f^*} \pm \mathrm{T.e.e^*} (\mathrm{mod\ s}) \tag{5}$$

In (5), $j = m^{\frac{e+1}{4}} = 1(\text{mod e})$, $T = m^{\frac{f+1}{4}} = 1(\text{mod f})$, $e^* = e^{-1}(\text{mod f})$ and $f^* = f^{-1}(\text{mod e})$. In this case, it is straightforward to derive e^* and f^* using the extended Euclidean algorithm (EA) since G (e, f) = 1.

Suppose that e and f are some two distinct odd prime numbers and s = e.f. The number of QRs modulo s is given in (6).

$$N = \frac{(e-1)(f-1)}{4} \tag{6}$$

Based on (6), the likelihood of any integer m being a QRM s is approximately 0.25.

3.2 The Proposed Protocol

The communicating entities that are involved in the proposed protocol include the Registration Authority (RA), the Gateway Node (GWN), the Ground Control Center (GCC) and the Unmanned Aerial Vehicles (UAVs). Figure 1 depicts the network architecture of the proposed protocol. As shown in this network, the UAVs exchange messages among themselves and these messages may then be forwarded on behalf of other UAVs. Before the onset of the message exchange process, all the UAVs are registered at the RA, after which they communicated to the GCC via the GWN. Here, the GWN contacted the RA to get updates regarding the registration details.

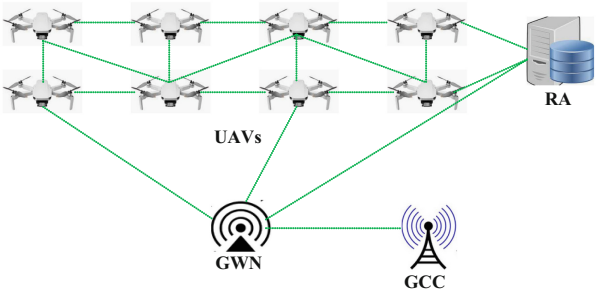

Fig.1. Network architecture.

However, the GWN and RA authentication is out of scope of the current work and hence the assumption made is that both the RA and the GWN are trusted entities. The GWN is particularly important where the GCC manages a large number of UAVs and the different UAVs could be grouped into a cluster and communicate via their respective GWNs. Table 1 presents the notations used in this paper.

The proposed protocol is executed in five major phases: parameter setting, registration, joining, UAV to GWN message signing - verification, and GWN to UAV message signing - verification phases. The details of these phases are discussed below.

Parameter Setting Phase: This phase involves the initialization of the security parameters that are utilized for the subsequent stages. It is executed in 3 steps as illustrated below.

Table 1. Symbols

Symbol	Description
ID_{UAV}	Unique identity of the UAV
ID_{GWN}	Unique identity of the GWN
SC_{UAV}	UAV secret code
SP_i	RA generated UAV secret parameters
E_k	Symmetric encryption using k
D_k	Symmetric decryption using k
T_M	Timestamp
j	Random integers
h(.)	Hashing operation
$\|\|$	Concatenation operation
$\oplus$	XOR operation

Step 1: The registration authority chooses two large distinct odd prime numbers A_1, A_2 and derives $B_1 = (A_1. A_2)$. Next, it chooses another two large distinct odd prime numbers A_3 and A_4 for each of the gateway nodes, before computing $B_2 = (A_3. A_4)$.
Step 2: The registration authority generates two prime numbers C_1 and C_2 for each of the unmanned aerial vehicle and then derives $B_3 = (C_1. C_2)$. Next, it transmits parameters $\{A_3, A_4\}$ and $\{ C_1, C_2\}$ to all GWNs and UAVs respectively.
Step 3: The RA selects some secure message authentication code (MAC) and one-way hashing function h(.) before publishing security parameters {MAC (.), B_1, B_2, B_3, h(.)}. At the same time, it privately stores security parameters $\{A_1, A_2\}$ in its database.

Registration Phase: In this phase, all the unmanned aerial vehicles are registered at the RA such that each of them is issued with some long-term secret keys. This phase is executed in 4 steps as detailed below.

Step 1: Each UAV generates its identity ID_{UAV} and secret code SC_{UAV} before sending registration request Reg_{Req} together with security parameters $\{ ID_{UAV}, SC_{UAV}\}$ to the RA through some secure channels.
Step 2: Upon receipt of Reg_{Req}, the registration authority generates a set of security parameters $SP = \{SP_1, SP_2, SP_3, \ldots.. SP_n\}$, where $SP_i \in SP$.
Step 3: The registration authority issues certificate cert $= \{SP_i, R_i, Q_i\}$ to UAV_i. Algorithm 1 illustrates the required steps for the generation of this certificate.

Algorithm 1: UAV→ GWN Certificate Generation

Begin
a) Input SP_i & initialize R_i to zero
b) Derive $m = h(SP_i, R_i)$
c) **IF** $m^{\frac{A_1-1}{2}} ! = 1 \pmod{A_1}$ and $m^{\frac{A_2-1}{2}} ! = 1 \pmod{A_2}$ **THEN:**
d) $R_i = R_i + 1$
e) **GoTo** step c
f) **ELSE:**
g) Derive modular square roots $n_{1,2,3,4}$ of $n^2 = m \pmod{B_1}$
h) Select the smallest square root as Q_i
i) **return** cert = (SP_i, R_i, Q_i)
END

As shown in Algorithm 1, the successful computation of the four square roots in step *g* requires knowledge of A_1 and A_2.

Step 4: The registration authority generates a UAV list U_L and stores parameters {SP_i, ID_{UAV}} in this list. This list is significant during the detection of malicious UAVs within the network. Finally, it sends security parameters {$h(ID_{UAV}, SC_{UAV})$, C_1, C_2, SP_i, R_i, Q_i} to the UAV over some secured channels.

Joining Phase: In the proposed protocol, the identity of the UAV is verified before being allowed to join the network. To accomplish this, the following 2 steps are followed:

Step 1: The UAV utilizes its unique identity ID_{UAV} and security code SC_{UAV} to derive $E = h(ID_{UAV}, SC_{UAV})$. Next, the resulting hash value E is transmitted securely to the RA.
Step 2: On receiving E, the RA uses its stored parameter set {ID_{UAV}, SC_{UAV}} to recomputed E^*. Next, the RA checks if $E^* \stackrel{?}{=} E$ such that the joining request is rejected if the two values are dissimilar. Otherwise, the UAV is legitimate and is permitted to join the network.

UAV → GWN Message Signing and Verification Phase: The three main procedures in the proposed protocol encompass Key Generation (KG), encryption and decryption. Basically, the KG step involves the sender selecting some two distinct large prime numbers *e* and *f* after which *s* is computed. This is followed by the publication of *s* but private storage of parameters *e* and *f*. During encryption, the sender composes message *msg* such that $msg.2^k$ is less than *s*. Afterwards, parameter $V = (msg.2^k)^2 \pmod{s}$ is derived and transmitted to the receiver. Upon receiving message V, the receiver derives four modular square roots of $q^2 = V \pmod{s}$ based on *e* and *f* as in (5). Finally, the original message *msg* is extracted from the modular square root with parameter *k*.

In the UAV network, messages M_i may be sent to the gateway node for subsequent transmission to the operator. During this transmission, it is important that UAV privacy is upheld, and these messages are securely delivered to their destinations. This is accomplished through message signing and verification using the 4 steps below.

Step 1: To start off message signing, the UAV generate random integer *j* and selects a single unused certificate $\text{cert}_U = \{SP_j, R_j, Q_j\}$. Here, $B_2^{\frac{1}{2}} < j < \frac{B_2}{2}$. It then chooses integer $k > 30$ and sets $T = 2^k$, where $2^{k-1} < B_2 < 2^k$.
Step 2: The UAV derives $Z = j^2.T^{-1} \pmod{B_2}$, $L = h(j)$, $X = MAC_L(ID_{GWN})$ and $Y = E_L(SP_j, R_j, Q_j, T_M, M_i)$.
Step 3: UAV constructs $UM = \{Z, X, Y\}$ and appends parameter set $\{SP_j, T_M\}$ in its malicious UAV list, M_{UL}. Here, the M_{UL} maintains a record of all pseudonyms of all revoked UAVs together with their respective timestamps. Finally, the UAV transmits final message UM to the GWN.
Step 4: After receiving UM from a particular UAV, the GWN validates this message to confirm whether the sending UAV is properly authenticated by the RA. To achieve this, Algorithm 2 is deployed. As shown in Algorithm 2, the GWN needs to derive four modular square roots as in step *a* followed by the computation of four hash values in step *b* which serve as the secret candidate keys.

To establish the precise secret key L, the GWN matches the received X with MAC operation in step *c*. In this case, the likelihood of having more than one candidate key matching is infinitesimal. In step *d*, the GWN deploys key L to decrypt parameter Y to obtain parameter set $\{SP_j, R_j, Q_j, T_M, M_i\}$. This is followed by the verification of timestamp T_M to thwart any packet replay attacks. To curb the re-use of any revoked certificate, the GWN extracts parameter set $\{SP_j, T_M\}$ from M_{UL} and one again validate timestamp T_M. In both cases, the verification process is terminated if T_M is invalid.

Algorithm 2: UAV→ GWN Message Verification

Begin
a) Derive modular square roots $n_{1,2,3,4}$ of $n^2 = Z.T \pmod{B_2}$
b) Compute $L_{1,2,3,4} = h(n_{1,2,3,4})$
c) Match received X with $X = MAC_{L_{1,2,3,4}}(ID_{GWN})$
d) Execute $D_L(Y) = (SP_j, R_j, Q_j, T_M, M_i)$
e) **IF** T_M is invalid **THEN:**
f) Terminate session
g) **ELSE:**
h) **IF** $Q_i^2 ! = h(SP_j, R_j) \pmod{B_1}$ **THEN:**
i) Terminate session
j) **ELSE:**
k) Permit data access

END

Otherwise, the GWN proceeds with the verification process by executing the check in step *h*. Provided that the authentication in step *h* is successful, the implication is that this UAV is legitimate and data access is allowed.
GWN → UAV Message Signing and Verification Phase: Upon sucessful message verification, the GWN examines message M_i to determine its legitimacy. If M_i is bogus, the GWN traces the particular UAV that sent this message and appends its SP_j together

with timestamp T_M in its M_{UL}. Otherwise, the GWN broadcasts M_i to all UAVs within its coverage area as described in step 1–5 below.

Step 1: The GWN derives some secret certificate as illustrated in Algorithm 3. As shown in Algorithm 3, the derivation of the four square roots in step *g* requires knowledge of A_3 and A_4. To thwart any masquerading attacks, each secret certificate is deployed only once.

Algorithm 3: GWN→ UAV Certificate Generation

Begin
a) Input ID_{GWN} & initialize R_i to zero
b) Derive $m = h(ID_{GWN}, R_i)$
c) **IF** $m^{\frac{A_3-1}{2}} = 1 \pmod{A_3}$ & $m^{\frac{A_4-1}{2}} = 1 \pmod{A_4}$ **THEN:**
d) $R_j = R_j + 1$
e) **GoTo** step c
f) **ELSE:**
g) Derive modular square roots $n_{1,2,3,4}$ of $n^2 = m \pmod{B_2}$
h) Select the smallest square root as Q_i
i) **return** cert $= (ID_{GWN}, R_i, Q_i)$
END

Step 2: Each time the GWN needs to share the received message M_j to all UAVs, it will need to sign this message before broadcasting it to all UAVs within its coverage area. To start off the signing process, the GWN selects some random integer $B_3^{\frac{1}{2}} < j^* < \frac{B_3}{2}$, where $2^{k-1} < B_3 < 2^k$. It then sets $T^* = 2^k$.
Step 3: The GWN derives $Z^* = j^{*2}.T^{*-1} \pmod{B_3}$, $L^* = h(j^*)$, $X^* = MAC_{L^*}(ID_{GWN})$ and $Y^* = E_{L^*}(ID_{GWN}, R_j, Q_j, T_M, M_j)$.
Step 4: GWN composes $GM = \{ID_{GWN}, Z^*, X^*, Y^*\}$ before broadcasting GM to all UAVs within its range.
Step 5: Upon receiving GM from the GWN, each UAV verifies message M_j in Y^* as described in Algorithm 4. The process begins by generating four square roots as in step *a* with the help of C_1 and C_2.

Algorithm 4: GWN→ UAV Message Verification

Begin

a) Derive modular square roots $n_{1,2,3,4}$ of $n^2 = Z^*.T^* \pmod{B_3}$
b) Compute $L^*_{1,2,3,4} = h(n_{1,2,3,4})$
c) Match received X^* with $X^* = MAC_{L^*_{1,2,3,4}}(ID_{GWN})$
d) Execute $D_{L^*}(Y^*) = (ID_{GWN}, R_j, Q_j, T_M, M_j)$
e) **IF** T_M is invalid **THEN:**
f) Terminate session
g) **ELSE:**
h) **IF** $Q_i^2 ! = h(ID_{GWN}, R_j) \pmod{B_2}$ **THEN:**
i) Terminate session
j) **ELSE:**
k) Accept & process M_j

END

This is followed by the computation of four hash values in step *b* to serve as secret keys. Next, the precise secret key L^* is established through matching the received ID_{GWN} and parameter X^* using the MAC operation in step *c*. This is followed by the decryption of parameter Y^* using key L^* to obtain the security parameters in step *d*. To curb any packet replay attacks, the timestamp verification in step *e* is executed. On the other hand, step *h* is carried out to thwart any masquerade attacks. Upon successful verification process, the UAV is assured that M_j was transmitted by a legitimate GWN and hence can accept and process its contents.

4 Security Analysis

The first part of this section presents the security analysis of the proposed protocol. This involves both formal analysis using Burrows–Abadi–Needham (BAN) logic, as well informal security analysis through some hypotheses that are formulated and proofed.

4.1 Formal Security Analysis

In this section, we deploy the widely adopted BAN logic to show that the proposed protocol attains the formulated authentications goals. To accomplish this, the BAN logic rules and notations in [4, 47] and [62] are utilized. In addition, the session –key rule is introduced during this analysis.

Session-key rule: $\frac{A|\equiv\#(\bar{B}), A|\equiv D|\equiv B}{A|\equiv A|\overset{L}{\leftrightarrow} D}$

During this analysis, the following four goals are formulated:

G_1: GWN $| \equiv (Z, X, Y)$

G_2: GWN $| \equiv$ GWN $\overset{j}{\leftrightarrow}$ UAV

G_3: UAV $| \equiv (ID_{GWN}, Z^*, X^*, Y^*)$

$\mathbf{G_4}$: UAV $| \equiv$ UAV $\overset{j^*}{\leftrightarrow}$ GWN

Based on the message exchanges in our protocol, two sets of messages are transmitted during the message signing and verification phase. These messages include UM = {Z, X, Y} sent from the UAV towards the GWN, and GM = $\{ID_{GWN}, Z^*, X^*, Y^*\}$ transmitted from the GWN to all the UAVs. In idealized form, these messages are represented as shown below.

UAV $\rightarrow$ GWN: {Z, X, Y}
$\{\langle j\rangle_T, (ID_{GWN})_j, \{SP_j, R_j, Q_j, T_M, M_i\}_j\}$
GWN $\rightarrow$ UAV: $\{ID_{GWN}, Z^*, X^*, Y^*\}$
$\{ID_{GWN}, \langle j^*\rangle_{T^*}, (ID_{GWN})_{j^*}, \{ ID_{GWN}, R_j, Q_j, T_M, M_j\}_{j^*}\}$

For effective evaluation of the proposed protocol, the following six initial assumptions (IAs) are made:

IA_1: GWN $| \equiv$ GWN $\overset{T}{\leftrightarrow}$ UAV
IA2: GWN $| \equiv$#TM
IA_3: GWN $| \equiv$ UAV $\Rightarrow\{SP_j, R_j, Q_j\}$
IA_4: UAV $| \equiv$ UAV $\overset{T^*}{\leftrightarrow}$ GWN
IA5: UAV $| \equiv$#TM
IA_6: UAV $| \equiv$ GWN $\Rightarrow\{ID_{GWN}, R_j, Q_j\}$

Thereafter, the idealized form of the proposed protocol is analyzed based on the BAN logic rules and initial assumptions. This analysis is executed step-wise in the BAN logic proofs (BLPs) below.

For the case of UAV $\rightarrow$ GWN: {Z, X, Y}:
$\{\langle j\rangle_T, (ID_{GWN})_j, \{SP_j, R_j, Q_j, T_M, M_i\}_j\}$

The application of seeing rule (SR) in the above idealized message yield BLP_1:

BLP_1: GWN $\triangleleft$ Z, X, Y: $\{\langle j\rangle_T, (ID_{GWN})_j, \{SP_j, R_j, Q_j, T_M, M_i\}_j\}$
According to the message-meaning rule (MMR), BLP_1 and IA_1, BLP_2 is yielded:
BLP_2: GWN $| \equiv$ UAV$|\sim\{j, (ID_{GWN})_j, \{SP_j, R_j, Q_j, T_M, M_i\}_j\}$
Based on the nonce-verification rule (NVR), fresh-promotion rule (FPR), BLP2 and IA2, BLP3 is obtained:
BLP_3: GWN $| \equiv$ UAV $| \equiv\{j, ID_{GWN}, SP_j, R_j, Q_j, T_M, M_i\}$
On the other hand, the application of the jurisdiction rule (JR) on both BLP_3 and IA_3 yields BLP_4:
BLP_4: GWN $| \equiv \{j, ID_{GWN}, \langle SP_j, R_j, Q_j\rangle_{B_{1\mapsto RA_i}}, T_M, M_i\}$, hence $\mathbf{G_1}$ is achieved.
According to IA_2, BLP_4 and session-key rule (SKR), BLP_5 is obtained.

BLP$_5$: GWN | $\equiv$ GWN $\overset{j}{\leftrightarrow}$ UAV, therefore $\mathbf{G_2}$ is attained.
For the case of GWN $\rightarrow$ UAV: $\{ID_{GWN}, Z^*, X^*, Y^*\}$
$\{ID_{GWN}, \langle j^* \rangle_{T^*}, (ID_{GWN})_{j^*}, \{ ID_{GWN}, R_j, Q_j, T_M, M_j\}_{j^*}\}$.
The application of SR in this idealized message results in BLP$_6$:
BLP$_6$: UAV $\triangleleft$ ID_{GWN}, Z^*, X^*, Y^*:$\{ID_{GWN}, \langle j^* \rangle_{T^*}, (ID_{GWN})_{j^*}, \{ID_{GWN}, R_j, Q_j, T_M, M_j\}_{j^*}\}$.
Based on BLP$_6$ and IA$_5$, NVR and FPR are applied to yield BLP$_7$:
BLP$_7$: UAV | $\equiv$ GWN|$\sim\{ID_{GWN}, j^*, (ID_{GWN})_{j^*}, \{ID_{GWN}, R_j, Q_j, T_M, M_j\}_{j^*}\}$
According to IA$_5$, NVR and FPR are applied on BLP$_7$ to get BLP$_8$:
BLP$_8$: UAV | $\equiv$ GWN | $\equiv\{j^*, ID_{GWN}, R_j, Q_j, T_M, M_j\}$
Based on BLP$_8$ and IA$_6$, jurisdiction rule (JR) is applied to yield BLP$_9$:
BLP$_9$: UAV | $\equiv$ $(ID_{GWN}, Z^*, X^*, Y^*)$, hence $\mathbf{G_3}$ is attained.
Finally, according to BLP$_9$ and IA$_5$, SR is applied to obtain BLP$_{10}$:
BLP$_{10}$: UAV | $\equiv$ UAV $\overset{j^*}{\leftrightarrow}$ GWN, achieving $\mathbf{G_4}$.

The successful attainment of all the four formulated security goals imply that the UAVs and the GWNs execute strong mutual authentication amongst themselves.

4.2 Informal Security Analysis

In this section, we show that the proposed protocol offers mutual authentication, misbehaving UAAV tracing, unlinkability and non-repudiation. In addition, it provides protection against forgery, impersonation, privacy leaks and packet replays. To achieve this, the following hypotheses are formulated and proofed.

Hypothesis 1: *The proposed protocol protects against forgery attacks.*

Proof: Suppose that an attacker is interested in capturing parameter sets $\{SP_j, R_j, Q_j, T_M, M_i\}$ or $\{ ID_{GWN}, R_j, Q_j, T_M, M_j\}$. To accomplish this, messages UM = {Z, X, Y} and GM = $\{ID_{GWN}, Z^*, X^*, Y^*\}$ must be intercepted. However, the decryption of Y and Y^* requires knowledge of secret key L which is unavailable to the adversary. If an attacker tries to forge messages UM and GM, these modifications are easily detected using Algorithm 2 and Algorithm 4 respectively.

Hypothesis 2: *Unlinkability is assured in the proposed scheme.*

Proof: In our scheme, message UM = {Z, X, Y} is generated at the UAV, where $Z = j^2.T^{-1} \pmod{B_2}$, $X = MAC_L\ (ID_{GWN})$ and $Y = E_L\ (SP_j, R_j, Q_j, T_M, M_i)$. Suppose that an adversary is interested in linking messages generated by the UAV. However, the incorporation of random integer j implies that message UM will be different for each session. If an attacker decrypts parameter Y, access to $\{SP_j, R_j, Q_j, T_M, M_i\}$ is obtained. However, certificate cert = $\{ SP_j, R_j, Q_j\}$ has never been used before and timestamp T_M is still fresh. As such, these parameters cannot be linked to any previously captured messages.

Hypothesis 3: *The proposed protocol offers mutual authentication.*

Proof: Suppose that an attacker has intercepted message UM = {Z, X, Y}, where $Z = j^2.T^{-1}$ (mod B_2), $X = MAC_L$ (ID_{GWN}) and $Y = E_L$ (SP_j, R_j, Q_j, T_M, M_i). However, without knowledge of both A_3 and A_4, and encryption key L, adversary cannot decrypt Y to access message M_i. Here, the correct computation of secret key L requires both A_3 and A_4 as evidenced in (3), and hence only legitimate GWN can decrypt it. In addition, upon receipt of message UM = {Z, X, Y} from a particular UAV, its authenticity is confirmed by the GWN using certificate cert = {SP_j, R_j, Q_j} in accordance with Algorithm 2. These certificates are only issued by the RA and without RA's valid parameters A_1 and A_2, an attacker is unable to generate these certificates. Similarly, when the GWN broadcasts message GM = {ID_{GWN}, Z^*, X^*,Y^*}, only UAVs with valid C_1 and C_2 can decrypt Y^* to access message M_j. The computation of secret key L^* requires knowledge of C_1 and C_2 which are only known to the legitimate UAVs. As such, without these parameters, an adversary cannot decipher Y^*. To authenticate the GWN, the UAVs utilizes certificate cert = {ID_{GWN}, R_j, Q_j} as described in Algorithm 4.

Hypothesis 4: *The proposed protocol assures message non-repudiation.*

Proof: The assumption made here is that a particular UAV has sent message UM = {Z, X, Y} but wants to deny having sent this message. However, each message sent by a UAV is signed by certificate cert = {SP_j, R_j, Q_j} that is issued by the RA. As such, a particular UAV cannot deny its own sent messages. Similarly, message GM = {ID_{GWN}, Z^*, X^*,Y^*} sent by the GWN is signed by its certificate cert = {ID_{GWN}, R_j, Q_j} and hence cannot be denied by a particular GWN.

Hypothesis 5: *Impersonation attacks are thwarted in the proposed scheme.*

Proof: To effectively masquerade as a UAV or GWN, messages UM = {Z, X, Y} and GM = {ID_{GWN}, Z^*, X^*, Y^*} must be generated respectively. However, this requires that an adversary have access to certificates cert = {SP_j, R_j, Q_j} and cert = {ID_{GWN}, R_j, Q_j}, in addition to parameter set {A_1, A_2} and {A_3, A_4}. Since these security tokens are only generated by the RA, any form of impersonation fails since fake certificates will be detected in accordance with Algorithm 2 and Algorithm 4.

Hypothesis 6: *The proposed protocol upholds identity privacy.*

Proof: During the registration phase, the RA assigns each UAV a set of secret parameters SP = {SP_1, SP_2, SP_3,….. SP_n} and equivalent certificates {SP_i, R_i}. During message transmission, a single unused secret parameter is chosen and incorporated in the sent message so as to conceal its identity. Consequently, it is infeasible for the UAV's real identity to be deciphered from the intercepted messages.

Hypothesis 7: *Replay attacks are prevented in our protocol.*

Proof: In the proposed protocol, message UM = {Z, X,Y} is sent from the UAV towards the GWN. On its part, the GWN transmits message GM = {ID_{GWN}, Z^*, X^*,Y^*}. Here, $Z = j^2.T^{-1}$ (mod B_2), L = h(j), $X = MAC_L$ (ID_{GWN}), $Y = E_L$ (SP_j, R_j, Q_j, T_M, M_i),

$Z^* = j^{*2}.T^{*-1}$ (mod B_3), $L^* = h(j^*)$, $X^* = MAC_{L^*}$ (ID_{GWN}) and $Y^* = E_{L^*}$ (ID_{GWN}, R_j, Q_j, T_M, M_j). Evidently, these messages incorporate timestamp T_M. During message verification in Algorithm 2 and Algorithm 4, the message freshness checks are executed. As such, any replayed message is easily detected in our protocol.

Hypothesis 8: *The proposed protocol offers traceability for misbehaving UAVs.*

Proof: During the registration phase, the certificates cert = {SP_i, R_i, Q_i} deployed for message signing and verification are issues by the RA. In addition, the RA generates secret parameters SP_j for each UAV. Since these parameters are related to the UAV real identities, it is only the RA that has knowledge of these identities. Upon generation of a single message UM = {Z, X,Y} using any available cert, the RA is able to relate this message to a particular secret parameter SP_i. Consequently, the RA can trace the real identity of the UAV. As such, any UAV misusing another UAV's real identity is easily identified and eliminated from the network.

5 Performance Evaluation

In typical security protocols, the execution time and bandwidth requirements are the widely adopted metrics for evaluating these protocols. As such, in this sub-section, the proposed protocol is evaluated using these metrics. In addition, the values obtained are compared with those of other related schemes.

Execution Time: During message signing and verification, the cryptographic operations executed include AES encryption (AE), Montgomery (M), AES decryption (AD), message authentication code (MA), modular square root (MS) and hashing (H) operations. The execution time (T) for these cryptographic operations are as follows: T_{AE} = 0.006 ms, T_M = 0.003 ms, T_{AD} = 0.003 ms, T_{MA} = 0.002 ms, T_{MS} = 0.076 ms and T_H = 0.001 ms. Based on the message signing and verification steps, single T_M, T_{AE}, T_{MA} and T_H operations are executed at the UAV and GWN and hence the total cost for signing is $2T_M$, $2T_{AE}$, $2T_{MA}$ and $2T_H$ operations. However, during message verification, $4T_{MA}$, $1T_M$, $5T_H$, $1T_{MS}$ and$1T_{AD}$ operations are carried out on the GWN and the UAVs. As such, the total cost for message verification is $8T_{MA}$, $2T_M$, $10T_H$, $2T_{MS}$ and $2T_{AD}$ operations. Consequently, the total execution time for signing and verification is: $4T_M + 2T_{AE} + 10T_{MA} + 12T_H + 2T_{AD} + 2T_{MS}$ operations. In overall, 0.214 ms are required for message signing and verification process as shown in Table 2.

Based on the results presented in Table 2, the scheme developed in [42] has the longest execution time followed by the schemes in [23, 25, 64] and the proposed protocol in that order. Given that the sensors in UAVs are resource limited, it is required that the authentication protocol be lightweight in terms of the cryptographic execution time. As such, the proposed protocol is the most applicable in the UAV sensor environment.
Bandwidth Requirement: In the proposed protocol, B_1, B_2 and B_3 are 512 bits in length while A_1, A_2, C_1, C_2, A_3 and A_4 are 256 bits each. On the other hand, HMAC operation using SHA-1, timestamp, hash function, AES encryption or decryption, and identity are

Table 2. Execution time

Scheme	Execution time (ms)
[64]	2.4345
[42]	34.3225
[25]	2.4769
[23]	2.4301
Proposed	0.214

160 bits, 32 bits, 160 bits, 256 bits and 32 bits in length respectively. During message signing and verification, messages UM = {Z, X,Y} and GM = {ID_{GWN}, Z^*, X^*,Y^*} are exchanged. Here, $Z = j^2.T^{-1} \pmod{B_2}$, $X = MAC_L$ (ID_{GWN}), $Y = E_L$ (SP_j, R_j, Q_j, T_M, M_i), $Z^* = j^{*2}.T^{*-1} \pmod{B_3}$, $X^* = MAC_{L*}$ (ID_{GWN}) and $Y^* = E_{L*}$ (ID_{GWN}, R_j, Q_j, T_M, M_j). The required bandwidth is then computed as follows:

UM = {Z, X,Y}: Z = 512 bits, X = 160 bits, Y = 256 bits,
hence UM is 928 bits long. On the other hand:
GM = {ID_{GWN}, Z^*, X^*,Y^*}: ID_{GWN} = 32 bits, Z^* = 512 bits, X^* = 160 bits, Y^* = 256 bits

As such, the total overhead for GM is 960 bits. Therefore, 1,888 bits are exchanged during the message signing and verification process, as shown in Table 3.

Table 3. Bandwidth requirements

Scheme	Bandwidth (bits)
[64]	1984
[42]	2528
[25]	1856
[23]	1696
Proposed	1888

Based on the graphs in Fig. 2, the protocol in [42] has the highest bandwidth requirements, followed by the protocols in [64], the proposed protocol, [25] and [23] in that order.

Although the scheme in [23] has the lowest bandwidth requirements, it is susceptible to de-synchronization attacks and cannot offer backward security. On the other hand, the protocol in [25] cannot offer backward and forward key secrecy, and has high communication costs. Consequently, although the proposed protocol has slightly higher bandwidth requirements than these protocols, it offers robust security features.

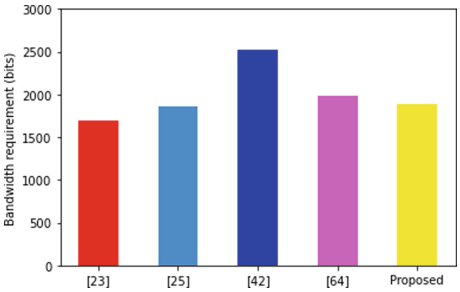

Fig.2. Bandwidth requirements.

6 Conclusion and Future Work

Many schemes have been developed for security and privacy enhancement in UAV networks. Majority of these schemes are based on PUF, ECC, PKC, blockchains, RSA certificates among other techniques. However, the noise in PUF-based schemes may lead to output bits being incorrect for some given challenges. On the other hand, the conventional authentication techniques based on dynamic keys, usernames or passwords offer low levels of security. In addition, RSA certification generates long session keys which are inefficient for UAV sensors. The dynamic topologies in UAVs owing to frequent mobility imply continuous identity authentication, hence the need for lightweight protocols. The proposed protocol has been demonstrated to fulfill this lightweight requirement, in addition to offering robust security and privacy protection. Future work lies in the deployment and evaluation of the proposed protocol in a real UAV communication environment so that the presented security and performance metrics can be validated.

Acknowledgement. This work is supported by Natural Science Foundation of Top Talent of SZTU (Grant number: 20211061010016) and National Natural Science Foundation of China under Grant 62072064.

References

1. Ozmen, M.O., Attila Yavuz, A.: Dronecrypt-an efficient cryptographic framework for small aerial drones. In: Prooceedings of IEEE Military Communications Conference (MILCOM), pp. 1–6. IEEE (2018)
2. Sun, J., et al.: A data authentication scheme for UAV ad hoc network communication. J. Supercomput. **76**(6), 4041–4056 (2017). https://doi.org/10.1007/s11227-017-2179-3
3. Giordan, D., et al.: The use of unmanned aerial vehicles (UAVs) for engineering geology applications. Bull. Eng. Geol. Env. **79**(7), 3437–3481 (2020). https://doi.org/10.1007/s10064-020-01766-2
4. Nyangaresi, V. O., Morsy, M.A.: Towards privacy preservation in internet of drones. In: 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), pp. 306–311. IEEE (2021)
5. Kwon, Y.M., Yu, J., Cho, B.M., Eun, Y., Park, K.J.: Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles. IEEE Access **6**, 43203–43212 (2018)

6. Teng, L., et al.: Lightweight security authentication mechanism towards UAV networks. In: 2019 International Conference on Networking and Network Applications (NaNA), pp. 379–384. IEEE (2019)
7. Hooper, M., et al.: Securing commercial Wifi based UAVs from common security attacks. In: Military Communications Conference (MILCOM), pp. 1213–1218. IEEE (2016)
8. Rodday, N.M., Schmidt, R.D.O., Pras, A.: Exploring security vulnerabilities of unmanned aerial vehicles. In: Network Operations and Management Symposium (NOMS), pp. 993–994. IEEE (2016)
9. Nyangaresi, V.O., Ogundoyin, S.O.: Certificate based authentication scheme for smart homes. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 202–207. IEEE (2021)
10. Bansal, G., Sikdar, B.: S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms. IEEE Trans. Veh. Technol. **70**(11), 12088–12100 (2021)
11. Srinivas, J., Das, A.K., Kumar, N., Rodrigues, J.J.: Tcalas: temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. IEEE Trans. Veh. Technol. **68**(7), 6903–6916 (2019)
12. Lei, Y., Zeng, L., Li, Y.X., Wang, M.X., Qin, H.: A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access **9**, 53769–53785 (2021)
13. Yahuza, M., Idris, M.Y.I., Wahab, A.W.A., Nandy, T., Ahmedy, I.B., Ramli, R.: An edge assisted secure lightweight authentication technique for safe communication on the Internet of drones network. IEEE Access **9**, 31420–31440 (2021)
14. Ever, Y.K.: A secure authentication scheme framework for mobile-sinks used in the Internet of drones applications. Comput. Commun. **155**, 143–149 (2020)
15. Lin, C., He, D., Kumar, N., Choo, K.K.R., Vinel, A., Huang, X.: Security and privacy for the Internet of drones: challenges and solutions. IEEE Commun. Mag. **56**(1), 64–69 (2018)
16. Nyangaresi, V.O., Petrovic, N.: Efficient PUF based authentication protocol for internet of drones. In: 2021 International Telecommunications Conference (ITC), pp. 1–4. IEEE (2021)
17. Yoon, K., Park, D., Yim, Y., Kim, K., Yang, S.K., Robinson, M.: Security authentication system using encrypted channel on UAV network. In: 2017 First IEEE International Conference on Robotic Computing (IRC), pp. 393–398. IEEE (2017)
18. Fang, D., Qian, Y., Hu, R.Q.: Security for 5g mobile wireless networks. IEEE Access **6**, 4850–4874 (2017)
19. Nyangaresi, V.O.: ECC based authentication scheme for smart homes. In: 2021 International Symposium ELMAR, pp. 5–10. IEEE (2021)
20. Aysu, A., Gulcan, E., Moriyama, D., Schaumont, P., Yung, M.: End-to-end design of a PUF-based privacy preserving authentication protocol. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 556–576. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48324-4_28
21. Gope, P., Lee, J., Quek, T.Q.S.: Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Trans. Inf. Forensics Secur. **13**(11), 2831–2843 (2018)
22. Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V., Rodrigues, J.J.P.C.: Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. IEEE Internet Things J. **6**(2), 3572–3584 (2019)
23. Ali, Z., Chaudhry, S.A., Ramzan, M.S., Al-Turjman, F.: Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles. IEEE Access **8**, 43711–43724 (2020)
24. Nyangaresi, V.O.: Hardware assisted protocol for attacks prevention in ad hoc networks. In: Miraz, M.H., Southall, G., Ali, M., Ware, A., Soomro, S. (eds.) iCETiC 2021. LNICSSITE, vol. 395, pp. 3–20. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90016-8_1

25. Dammak, M., Boudia, O.R.M., Messous, M.A., Senouci, S.M., Gransart, C.: Token-based lightweight authentication to secure IoT networks. In: Proceedings of 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1–4. IEEE (2019)
26. Li, T., Ma, J., Ma, X., Gao, C., Zhang, J.: Lightweight secure communication mechanism towards UAV networks. In: Proceedings of IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2019)
27. Shi, X., Xiao, D.: A reversible watermarking authentication scheme for wireless sensor networks. Inf. Sci. **240**(11), 173–183 (2013)
28. Nicanfar, H., Jokar, P., Leung, V.C.: Smart grid authentication and key management for unicast and multicast communications. In: 2011 IEEE PES Innovative Smart Grid Technologies, pp. 1–8. IEEE (2011)
29. Nyangaresi, V.O., Rodrigues, A.J., Taha, N.K.: Mutual authentication protocol for secure VANET data exchanges. In: Perakovic, D., Knapcikova, L. (eds.) FABULOUS 2021. LNICSSITE, vol. 382, pp. 58–76. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-78459-1_5
30. Pu, C., Li, Y.: Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. In: Proceedings of EEE International Symposium on Local and Metropolitan Area Networks (LANMAN), pp. 1–6. IEEE (2020)
31. Chen, L., Qian, S., Lim, M., Wang, S.: An enhanced direct anonymous attestation scheme with mutual authentication for network connected UAV communication systems. China Commun. **15**(5), 61–76 (2018)
32. Asokan, N., et al.: Seda: scalable embedded device attestation. In: Proceedings of the 22nd SIGSAC Conference on Computer and Communications Security, pp. 964–975. ACM (2015)
33. Ibrahim, A., Sadeghi, A.R., Tsudik, G., Zeitouni, S.: Darpa: device attestation resilient to physical attacks. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 171–182. ACM (2016)
34. Zhang, Y., He, D., Li, L., Chen, B.: A lightweight authentication and key agreement scheme for Internet of drones. Comput. Commun. **154**, 455–464 (2020)
35. Lee, K., Nieto, J.G., Boyd, C.: A state-aware RFID privacy model with reader corruption. In: Xiang, Y., Lopez, J., Kuo, C.-C. J., Zhou, W. (eds.) CSS 2012. LNCS, vol. 7672, pp. 324–338. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-35362-8_25
36. Nyangaresi, V.O., Abduljabbar, Z.A., Al Sibahee, M.A., Abduljaleel, I.Q., Abood, E.W.: Towards security and privacy preservation in 5G networks. In: 2021 29th Telecommunications Forum (TELFOR), pp. 1–4. IEEE (2021)
37. Guan, T., Chen, Y.: A node clone attack detection scheme based on digital watermark in WSNs. In: IEEE International Conference on Computer Communication and the Internet, pp. 257–260. IEEE (2016)
38. Liang, W., Xie, S., Long, J., Li, K.C., Zhang, D., Li, K.: A double PUF based RFID identity authentication protocol in service-centric internet of things environments. Inf. Sci. **503**, 129–147 (2019)
39. Chamola, V., Hassija, V., Gupta, V., Guizani, M.: A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. IEEE Access **8**, 90225–90265 (2020)
40. Pandey, S., Deyati, S., Singh, A., Chatterjee, A.: Noise-resilient SRAM physically unclonable function design for security. In: IEEE 25th Asian Test Symposium, ATS, pp. 55–60. IEEE (2016)
41. Nyangaresi, V.O., Moundounga, A.R.A.: Secure data exchange scheme for smart grids. In: 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), pp. 312–316. IEEE (2021)
42. Challa, S., et al.: Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access **5**, 3028–3043 (2017)

43. Tai, W.L., Chang, Y.F., Li, W.H.: An IoT notion-based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. J. Inf. Secur. Appl. **34**, 133–141 (2017)
44. Yan, Q., Gong, Q., Deng, F.A.: Detection of DDoS attacks against wireless SDN controllers based on the fuzzy synthetic evaluation decision making model. Adhoc Sens. Wirel. Netw. **33**, 275–299 (2016)
45. Benzarti, S., Triki, B., Korbaa, O.: Privacy preservation and drone authentication using id-based signcryption. In: SoMeT, pp. 226–239 (2018)
46. Rupa, C., Srivastava, G., Gadekallu, T.R., Maddikunta, P.K.R., Bhattacharya, S.: Security and privacy of UAV data using blockchain technology. J. Inf. Secur. Appl. **55**, 102670 (2020)
47. Nyangaresi, V.O.: Lightweight key agreement and authentication protocol for smart homes. In: 2021 IEEE AFRICON, pp. 1–6. IEEE (2021)
48. Püllen, D., Anagnostopoulos, N.A., Arul, T., Katzenbeisser, S.: Using implicit certification to efficiently establish authenticated group keys for in-vehicle networks. In: Proceedings of IEEE Vehicular Networking Conference (VNC), pp. 1–8. IEEE (2019)
49. Bansal, G., Naren, N., Chamola, V.: Rama: real-time automobile mutual authentication protocol using puf. In: Proceedings of IEEE International Conference on Information Networking (ICOIN), pp. 265–270. IEEE 2020
50. Bansal, G., Naren, N., Chamola, V., Sikdar, B., Kumar, N., Guizani, M.: Lightweight mutual authentication protocol for v2g using puf. IEEE Trans. Veh. Technol. **69**(7), 7234–7246 (2020)
51. Barman, S., Shum, H.P.H., Chattopadhyay, S., Samanta, D.: A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. IEEE Access **7**, 12557–12574 (2019)
52. Ali, Z., et al.: Itssaka-ms: an improved three-factor symmetric key based secure aka scheme for multi-server environments. IEEE Access **8**, 107993–108003 (2020)
53. Semal, B., Markantonakis, K., Akram, R.N.: A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. In: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), pp. 1–8. IEEE (2018)
54. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: Machine learning protocol for secure 5G handovers. Int. J. Wirel. Inf. Netw.**29**, 1–22 (2022)
55. Tian, Y., Yuan, J., Song, H.: Efficient privacy-preserving authentication framework for edge-assisted internet of drones. J. Inf. Secur. Appl. **48**, 102354 (2019)
56. Turkanovi´c, M., Brumen, B., Hölbl, M.: A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad. Hoc Netw. **20**, 96–112 (2014)
57. Farash, M.S., Turkanovi´c, M., Kumari, S., Hölbl, M.: An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Netw. **36**, 152–176 (2016)
58. Bringer, J., Chabanne, H., Icart, T.: Improved privacy of the tree-based hash protocols using physically unclonable function. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 77–91. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85855-3_6
59. Amin, R., Islam, S.H., Biswas, G.P., Khan, M.K., Leng, L., Kumar, N.: Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Comput. Netw. **101**, 42–62 (2016)
60. Jiang, Q., Zeadally, S., Ma, J., He, D.: Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks. IEEE Access **5**, 3376–3392 (2017)
61. Yao, X., Han, X., Du, X.: A light-weight certificate-less public key cryptography scheme based on ECC. In: Proceedings of 23rd International Conference on Computer Communications and Networks (ICCCN), pp. 1–8. IEEE (2014)

62. Nyangaresi, V.O., Rodrigues, A.J.: Efficient handover protocol for 5G and beyond networks. Comput. Secur. **113**, 102546 (2022)
63. Seo, S.H., Won, J., Bertino, E.: pCLSC-TKEM: a pairing free certificateless signcryption-tag key encapsulation mechanism for a privacy-preserving IoT. Trans. Data Priv. **9**(2), 101–130 (2016)
64. Das, A.K.: A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Netw. Appl. **9**(1), 223–244 (2014). https://doi.org/10.1007/s12083-014-0324-9
65. Guo, C., Chang, C.C., Chang, S.C.: A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications. I.J Netw. Secur. **20**(2), 323–331 (2018)