Ocean Engineering 250 (2022) 110894

Contents lists available at ScienceDirect

Ocean Engineering

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

A resource friendly authentication scheme for space–air–ground–sea integrated Maritime Communication Network

Muhammad Asghar Khan [a], Bander A. Alzahrani [b], Ahmed Barnawi [b], Abdullah Al-Barakati [b], Azeem Irshad [c], Shehzad Ashraf Chaudhry [d,*]

[a] Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan
[b] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[c] Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan
[d] Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey

ARTICLE INFO

Keywords:
MaritimE Communication Network
Internet of Things (ioT)
Security
Authentication
ECC
6G/IoT

ABSTRACT

Recently, the demand for a faster , low-latency, and full-coverage Maritime Communication Network (MCN) has gained attention as marine operations have increased substantially. Using modern information network technologies and integrating space, air, ground, and sea network segments, MCN may be able to offer worldwide coverage and diverse Quality-of-Service (QoS) provisioning. These network segments are expected to provide not only traditional communication services, but also processing, caching, sensing, and control capabilities when linked via Sixth Generation (6G) mobile networks. However, this development in infrastructure growth is subjected to new security and privacy concerns due to open links, moving nodes, and diverse collaborative algorithms. In this paper, we propose an improved and resource friendly authentication scheme for the space–air–ground–sea integrated maritime communication network using Elliptic Curve Cryptography (ECC). To validate the security hardness of the proposed scheme, formal security assessment method such as Random Oracle Model (ROM) is used. Finally, comparisons with relevant authentication schemes are provided in terms of computation and communication costs. The findings support the viability of the proposed scheme.

1. Introduction

In recent years, the maritime industry has seen significant expansion due to the rapid increase in marine activities such as shipping, offshore aquaculture, and oceanic mineral exploration (Wei et al., 2021). This development leads to a rising demand for high-speed and ultra-reliable Maritime Communication Network (MCN) to connect the growing number of vessels, offshore platforms, buoys, and other maritime infrastructure (Wang et al., 2015; Xia et al., 2020; Zhang et al., 2020). For example, safe navigation of all vessels requires maritime information and operational data. Similarly, offshore drilling platforms require real-time operational data communication. In addition to exchanging information using text and voice, maritime rescue operation often requires real-time video streaming for vessel-to-vessel and vessel-to-shore coordination. Utilizing modern information network technologies and interconnecting space, air, ground and sea network segments, a global MCN can be established. Satellites, in particular, can offer seamless connectivity to seas, while air segment networks can enhance capacity for covered areas with high service demands, and densely deployed ground and sea segment systems can support high data rate access (Liu et al., 2018). Meanwhile, satellite operators are developing a multi-layer airborne component system that comprises the High Altitude Platform System (HAPS) to provide cost-effective communication services over the oceans. In addition, the low-cost, high-performance drones have become a vital facilitator and a key vertical component of the future 6G ecosystem (Motlagh et al., 2016; Guan et al., 2021; Huo et al., 2020). When connected via future 6G wireless communications for MCN, the integration of various network segments would provide numerous benefits. The future 6G-enabled space–air–ground–sea Integrated MCN will include satellites that help achieve global coverage for maritime communications, and drones that may operate as a relay, as shown in Fig. 1. HAPS, which are often positioned above the stratosphere, can offer better coverage and collaborate with satellites to establish more trustworthy MCN, particularly when satellite communications are hampered by bad weather. The vessels are equipped with a range of Internet of Things (IoT) sensors that assist in operations. They are also dedicated to collecting and disseminating event-related messaging. Finally, the Ground Control

* Corresponding author.
E-mail addresses: sashraf@gelisim.edu.tr, ashraf.shehzad.ch@gmail.com (S.A. Chaudhry).

https://doi.org/10.1016/j.oceaneng.2022.110894
Received 22 November 2021; Received in revised form 13 January 2022; Accepted 18 February 2022
Available online 8 March 2022

Station (GCS) is responsible for maintaining overall control of the maritime system. This expansion in infrastructure, on the other hand, poses new security and privacy concerns due to open wireless connectivity, movable nodes, and widespread deployment of IoT devices onboard the vessels. If there are no countermeasures to ensure data security and privacy requirements, attackers may cause problems throughout the network and can leak sensitive data. The Global Positioning System (GPS) spoofing attack (Arteaga et al., 2019; Banerjee et al., 2019a,b; Bera et al., 2020; Canetti and Krawczyk, 2002; Challa et al., 2017, 2020; Chaudhry et al., 2020, 2021; Das et al., 2018, 2019; Dolev and Yao, 1983; Ever, 2020; Farash et al., 2016; Guan et al., 2021; Guo et al., 2019), in which an attacker uses GPS signals, is an example of a serious security risk violating the privacy of MCN. In this technique, an attacker sends a targeted vessel fake GPS signals that are slightly stronger than real GPS signals to steer them away from their planned destination and toward the attacker's preferred position. As a result, effective security measures have become one of most significant criteria for MCN. This necessitates the use of authentication scheme that allows all of these entities to securely communicate real-time data. A well-designed authentication mechanism may greatly decrease the likelihood of data being compromised. With the aforementioned security challenges in mind, in this article, an improved and resource-friendly authentication scheme has been proposed. When compared to Rivest–Shamir–Adleman (RSA) and bilinear pairing methods, the scheme uses the concept of Elliptic Curve Cryptography (ECC) and is distinguished by smaller key length (Khan et al., 2021). Importantly, it provides the security features in an uncompromising way. The following noteworthy characteristics characterize the research work:

1. We propose an improved and resource-friendly authentication scheme for a space–air–ground–sea integrated MCN.
2. The proposed scheme employs the ECC, which has the same level of security as RSA and bilinear pairing but with a smaller key size.
3. The proposed scheme is shown to be resistant against various attacks through the formal security analysis method i.e Random Oracle Model (ROM).
4. Finally, a thorough comparative analysis is carried out to determine the feasibility of the proposed scheme in comparison to its counterpart schemes. The results reveal that the proposed method has a better security-to-efficiency tradeoff.

1.1. Organization of the paper

The organization of the article is set out as follows. The related work on authentication and key agreement schemes is presented in Section 1.2. We go through system models in Section 2, which also includes network and threat models. In Section 3, the proposed model and algorithm are defined. Section 4, on the other hand, provides the proposed scheme's security analysis. In addition, we discuss performance analysis in Section 5. The conclusion is presented in Section 6.

1.2. Related work

The major security measures for MCN rely on cryptographic concepts to ensure authenticity, confidentiality and integrity. A well-designed data security strategy may greatly decrease the likelihood of data being compromised. However, the topic of security and privacy problems for maritime networks has not received ample attention in the scholarly literature thus far. We found various ECC-based authentication schemes in the literature that may be used to investigate the data protection problems for MCN. Turkanovi/'c et al. (2014) proposed a lightweight key-agreement scheme that allows a distant user to securely share a session key with a sensor node and offer mutual authentication between the user, sensor node, and gateway node. Banerjee et al. (2019a) revealed that the scheme proposed in Turkanovi/'c et al. (2014) is vulnerable to different attacks such as sensor node acquisition, Denial-of-Services (DoS), insecure login phase, and other similar attacks. After that, Banerjee et al. proposed an improved scheme to solve the issues. Farash et al. (2016) also demonstrated that Turkanovic et al.'s scheme is vulnerable to numerous cryptographic attacks. Farash et al. then proposed viable solutions in the form authentication scheme with three-party settings that may be used in wireless sensor networks. Challa et al. (2017) proposed a signature-based authentication scheme for three-party IoT environments in 2017. Later in 2020, Challa et al. (2020) proposed another authentication scheme for securing three-party settings in cloud-based IoT systems. However, Chaudhry et al. (2020) claimed that both the schemes presented in Challa et al. (2017, 2020) were incorrect and inapplicable in real-world situations.

Das et al. (2018) presented another solution to secure industrial IoT in three-party settings in 2018. Hussain and Chaudhry (Hussain and Chaudhry, 2019) pointed out some critical flaws in Das et al.'s scheme. Furthermore, Das et al. (2019), Malani et al. (2019), and Odelu et al. (2017) offer a two-phase approach that aims for a secure communication paradigm between two sensing nodes. Node authentication, key agreement, and the idea of ECC are all part of it. The high expenses and two-party settings are an obvious disadvantages of such schemes presented in Das et al. (2019), Dolev and Yao (1983), Ever (2020), Farash et al. (2016), Guan et al. (2021), Guo et al. (2019), Huo et al. (2020), Hussain and Chaudhry (2019), Hussain et al. (2021), Kilinc and Yanik (2013), Liu et al. (2018), Malani et al. (2019), Motlagh et al. (2016), Odelu et al. (2017). Recently, Hussain et al. (2021) proposed an authentication scheme that uses the concept of ECC to secure communication between a user and a drone flying in a defined flying zone. Wazid et al. (2019a) presented a scheme of authentication key exchange for fog computing called SAKA-FC. However, Ali et al. (2021) assessed and revealed that the SAKA-FC has several serious flaws. The authors also proposed an improved authentication scheme to address these issues while maintaining the system's merits. We propose an improved and resource-friendly authentication scheme for MCN as a coping mechanism to solve the aforementioned shortcomings. The scheme, which is based on ECC, has shown to be considerably more secure and efficient.

Table 1
Notations guide.

Symbols	Representations
CS_k, V_i	Control station, Vessel
HAP_j	High Altitude Platform
I_{ck}, I_{hj}, I_{vi}	Identities of CS_k, HAP_j, V_i
$E_p(a,b), P$	Elliptic Curve, An EC Point
s_{ck}, $Q_{ck} = s_{ck}P$	Private/public key pair of CS_k
s_{hj}, Q_{hj}	Private/public key pair of HAP_j
K_{HC}	Shared secret among HAP_j and CS_k
s_{vi}, Q_{vi}	Private/public key pair of V_i
K_{VC}	Shared secret among V_i and CS_k
$\overline{I}_{vi}$	V_i's Pseudo-Identity
T_{vi}, t_{hj}, t_{ck}	Timestamps of V_i, HAP_j, CS_k
r_{vi}, r_{hj}, r_{ck}	Random numbers of V_i, HAP_j, CS_k
$H(.), h(.)$	Two Hash functions
$E_x(A)$	Block encryption of A using x

2. System models

Some important notations used in this paper are defined in Table 1 and to describe the operation and implementation of the proposed scheme, details about network and threat models are as follows:

2.1. Network model

We propose an integrated space–air–ground–sea maritime communication network that includes IoT-enabled vessels, drones, the High Altitude Platform System (HAPS), satellites, and a control station (CS).

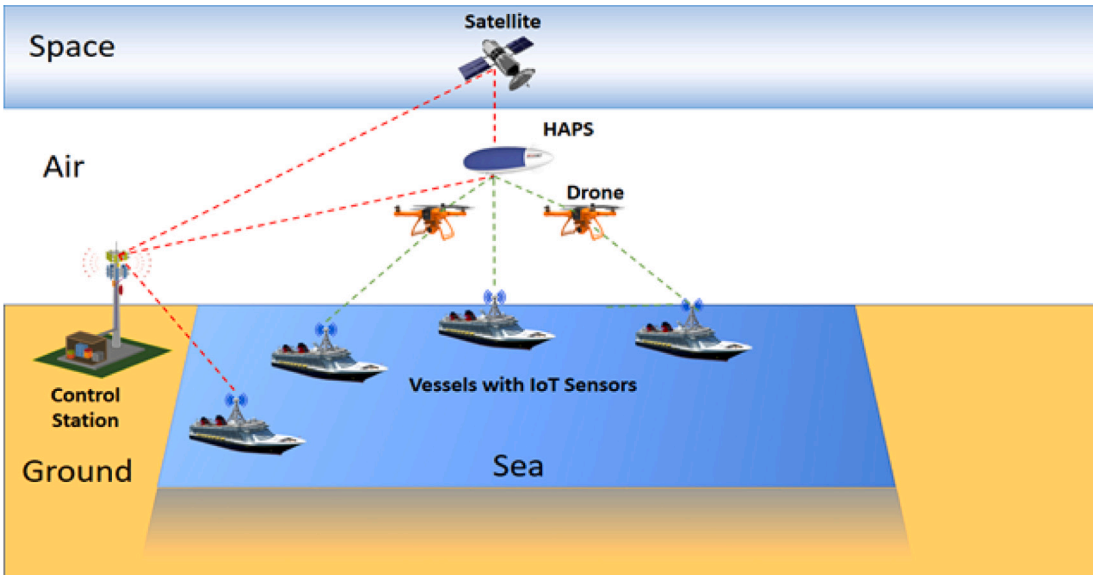

Fig. 1. Sample architecture for 6G-IoT enabled MCN.

IoT devices aid in better decision-making for operations such as route and delivery planning, cargo scheduling and management, and weather analysis for vessels. These devices are also used to gather and share occurrence messages. A drone with cameras, an Inertial Measurement Unit (IMU), sensors, and a GPS unit may fly beside the designated vessel. Satellites assist in the coverage of maritime communications across the globe. Furthermore, HAPS provides greater coverage/relay and links with satellites, allowing for the formation of more trustworthy maritime communication networks, particularly when satellite communications are hindered by severe weather. HAPS may use 6G, and extra equipment on the drones and vessels is not required.

2.2. Threat model

The widely used "Canetti and Krawczyk's adversary model (CK-adversary model)" is a de facto standard for modeling authentication methods, according to studies (Canetti and Krawczyk, 2002). The proposed method employs the Dolev–Yao (DY) paradigm, which incorporates insecure public channel communication and participant distrust (Dolev and Yao, 1983). As a result, a hostile attacker can simply interfere and access the contents of the conversations. The attacker may also compromise the session states, secret parameters, and other credentials, according to the CK-attack paradigm.

3. Proposed scheme

In this section, we put forward our novel scheme for Space–Air–Ground–Sea Integrated Maritime Communication Network. The detail of each phase is listed below:

3.1. Initialization

For initialization, the CS selects an elliptic curve $E_p(a,b)$ and a point P and $h, H : \{0,1\}^* \rightarrow Z_q^*$ the two hash functions, along with $h(..)$ as a one way secure hash function. CS now selects/computes the key pair $\{s_{ck} \in z_q^*, Q_{ck} = s_{ck}P\}$ and announces $\{P, q, h(..), Q_{ck}\}$ publicly and keeps s_T secret.

3.2. HAP registration

During this phase the HAP is registered and for this purpose, the CS selects its identity I_{hj} and private key say s_{hj}. Then, it computes publicizes its public key $Q_{hj} = s_{hj}P$. In addition, the CS computes a shared key among the CS and HAP as $K_{HC} = h(s_{ck} \parallel I_{hj})$. Finally, the CS hands over $\{s_{hj}, K_{HC}\}$ pair to HAP and publishes Q_{hj}.

3.3. Vessel registration

This phase is initiated independently by each vessel (V_i) by selecting and sending its identity I_{vi} to CS, which computes $Q_{vi} = kP$, $s_{vi} = h(I_{vi})s_{ck} + k$, where k is a random integer generated by CS. Now, the CS computes shared secret $K_{VC} = h(s_{ck} \parallel I_{vi})$ and sends back $\{s_{vi}, K_{VC}\}$ to V_i and publishes Q_{vi}.

3.4. Authentication phase

This process is initiated by a vessel V_i rightly when it wants to furnish an authentication round with CS_k through the support of the concerned HAP. The process is depicted in Fig. 2 and explained as follows:

Step VHC1: $\boldsymbol{V_i \rightarrow HAP_j}$: $\{\boldsymbol{M_1}\}$ The vessel V_i after randomly selecting $r_{vi} \in Z_q^*$, computes $\alpha_{vi} = r_{vi}P$, $\overline{I}_{vi} = I_{vi} \oplus r_{vi}Q_{hj}$ and sends $M_1 = \{\alpha_{vi}, \overline{I}_{vi}\}$ to HAP_j.

Step VHC2: $\boldsymbol{HAP_j \rightarrow V_i}$: $\{\boldsymbol{M_2}\}$ The HAP_j on receiving M_1 extract real identity of the vessel by adopting following: $I_{vi} = \overline{I}_{vi} \oplus s_{hj}\alpha_{vi}$. Now HAP_j after randomly selecting $r_{hj} \in Z_q^*$ computes $\alpha_{hj} = r_{hj}P$ and $\beta_{hj} = r_{hj}(Q_{vi} + h(I_{vi})Q_{ck}) = (x_\beta, y_\beta)$. Now, HAP_j generates current timestamp t_{hj}, computes $H_{hj}^1 = h(x_\beta \parallel \alpha_{vi} \parallel \alpha_{hj} \parallel \beta_{hj} \parallel I_{vi} \parallel t_{hj})$ and sends $M_2 = \{t_{hj}, \alpha_{hj}, H_{hj}^1\}$ to V_i.

Step VHC3: $\boldsymbol{V_i \rightarrow HAP_j}$: $\{\boldsymbol{M_3}\}$ The V_i on receiving M_2, first confirms the freshness of the timestamp t_{hj}, and in case freshness is proved, V_i computes $\beta_{vi} = s_{vi}\alpha_{hj} = (x_\beta, y_\beta)$ and checks the validity of M_3 and the sender HAP_j by validating $H_{hj}^1 \stackrel{?}{=} h(x_\beta \parallel \alpha_{vi} \parallel \alpha_{hj} \parallel \beta_{hj} \parallel I_{vi} \parallel t_{hj})$. In case of successful validation, V_i after randomly selecting t_{vi} computes $H_{vi}^1 = H(y_\beta \parallel \alpha_{vi} \parallel \alpha_{hj} \parallel \beta_{vi} \parallel t_{vi})$, $H_{vi}^2 = h(I_{vi} \parallel K_{VC} \parallel \alpha_{vi} \parallel \beta_{vi} \parallel t_{vi})$ and sends $M_3 = \{H_{vi}^1, H_{vi}^2 t_{vi}\}$ to HAP_j.

Step VHC4: $\boldsymbol{HAP_j \rightarrow CS_k}$: $\{\boldsymbol{M_4}\}$ The HAP_j on receiving M_3, first confirms the freshness of the timestamp t_{vi}, and in case freshness is proved, HAP_j checks the validity of M_3 and the sender V_i by validating $H_{vi}^1 \stackrel{?}{=} H(y_\beta \parallel \alpha_{vi} \parallel \alpha_{hj} \parallel \beta_{vi} \parallel t_{vi})$. In case of successful validation, HAP_j generates t_{hj}^2, computes $C_{hj} = E_{K_{HC}}(I_{vi} \parallel \alpha_{vi} \parallel \beta_{vi} \parallel t_{vi} \parallel t_{hj^2})$, $H_{hj}^2 = h(\alpha_{vi} \parallel \beta_{vi} \parallel t_{vi} \parallel t_{hj}^2 \parallel K_{HC})$ and sends $M_4 = \{I_{hj}, C_{hj}, H_{hj}^2, H_{vi}^2, t_{hj}^2\}$ to CS_k.

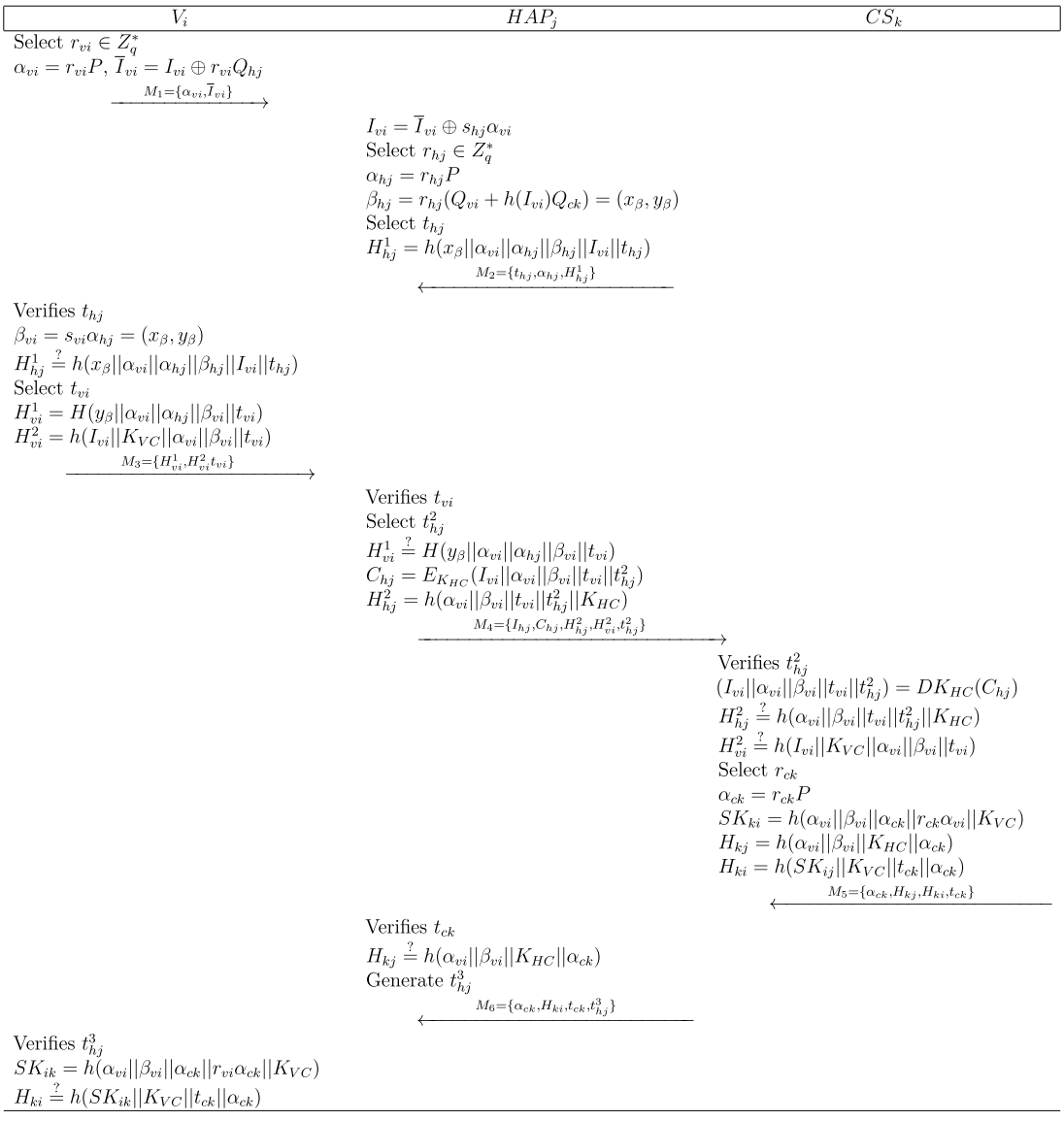

Fig. 2. Proposed Scheme.

Step VHC5: $\boldsymbol{CS_k \rightarrow HAP_j}$: $\{\boldsymbol{M_5}\}$ The CS_k on receiving M_4, first confirms the freshness of the timestamp t_{hj}^2, and in case freshness is proved, CS_k decrypts C_{hj} using shared key K_{HC} among HAP_j and CS_k to get $(I_{vi} \parallel \alpha_{vi} \parallel \beta_{vi} \parallel t_{vi} \parallel t_{hj}^2) = DK_{HC}(C_{hj})$. Now, CS_k, HAP_j and V_i check the validity of M_4, $H_{hj}^2 \stackrel{?}{=} h(\alpha_{vi} \parallel \beta_{vi} \parallel t_{vi} \parallel t_{hj}^2 \parallel K_{HC})$ $H_{vi}^2 \stackrel{?}{=} h(I_{vi} \parallel K_{VC} \parallel \alpha_{vi} \parallel \beta_{vi} \parallel t_{vi})$, respectively. In case of successful validation of both V_i and HAP_j, the CS_k after randomly selecting r_{ck} computes $\alpha_{ck} = r_{ck}P$, $SK_{ki} = h(\alpha_{vi} \parallel \beta_{vi} \parallel \alpha_{ck} \parallel r_{ck}\alpha_{vi} \parallel K_{VC})$, $H_{kj} = h(\alpha_{vi} \parallel \beta_{vi} \parallel K_{HC} \parallel \alpha_{ck})$ and $H_{ki} = h(SK_{ij} \parallel K_{VC} \parallel t_{ck} \parallel \alpha_{ck})$. Now, CS_k sends $M_5 = \{\alpha_{ck}, H_{kj}, H_{ki}, t_{ck}\}$ to HAP_j.

Step VHC6: $\boldsymbol{HAP_j \rightarrow V_i}$: $\{\boldsymbol{M_6}\}$ The HAP_j on receiving M_5 first confirms the freshness of the timestamp t_{ck}, and in case freshness is proved, HAP_j and the sender CS_k confirm the validity of M_5 and $H_{kj} \stackrel{?}{=} h(\alpha_{vi} \parallel \beta_{vi} \parallel K_{HC} \parallel \alpha_{ck})$, respectively. In case of successful verification of M_5 and CS_k, the HAP_j generate t_{hj}^3 and sends $M_6 = \{\alpha_{ck}, H_{ki}, t_{ck}, t_{hj}^3\}$ to V_i.

Step VHC7: The V_i on receiving M_6, first confirms the freshness of the timestamp t_{hj}^3, and in case freshness is proved, V_i computes the session key $SK_{ik} = h(\alpha_{vi} \parallel \beta_{vi} \parallel \alpha_{ck} \parallel r_{vi}\alpha_{ck} \parallel K_{VC})$. Finally, the V_i checks $H_{ki} \stackrel{?}{=} h(SK_{ik} \parallel K_{VC} \parallel t_{ck} \parallel \alpha_{ck})$. In case, the verification is successful, V_i keeps SK_{ik} as session key for all subsequent communication and considers CS_k as authenticated.

4. Security analysis

This section presents formal and informal security analysis in the following:

4.1. Formal security analysis

This section proves and analyzes the security properties of contributed authentication model. Before the demonstration of formal analysis we present few preliminaries related to collision resistant one way hash function, DL and CDH problems. Later, we prove the security features of proposed model by employing universally renowned Real-Or-Random (ROR) model.

4.1.1. Preliminaries

The security of our scheme relies on the hardness of one way hash function, Computational Diffie Hellman (CDH) problem, and Discrete Logarithm (DL) problem.

Definition 1 (*Cryptographic Hash Function*)**.** The deterministic, one-way collision resistant hashing function $H : \{0,1\}^* \rightarrow \{0,1\}^l$ takes input of a string with random length, and produces an output with fixed length l. If $Adv_{\mathcal{A}}^{H_s}(t)$ be the advantage of attacker $\mathcal{A}$ for finding hash-based collisions in time t, then

$$Adv_{\mathcal{A}}^{H_s}(t) = Pr[(\eta_1, \eta_2) \Leftarrow_R \mathcal{A} : \eta_1 \neq \eta_2 \wedge \ h(\eta_1) = h(\eta_2)]. \quad (1)$$

where $(\eta_1, \eta_2) \Leftarrow_R \mathcal{A}$ illustrates that η_1 and η_2 are selected on random basis by the attacker. An (ϕ, t)-attacker $\mathcal{A}$ breaking the collision resistance property of $H_s(\cdot)$ suggests that $Adv_{\mathcal{A}}^{H_s}(t) \leq \phi$ assuming the maximum runtime t.

Definition 2 (*Discrete Logarithm (DL) Problem*)**.** Given two randomly defined points A, $B \epsilon G$, where $A = aP$, $a \epsilon Z_q^*$, and $Z_q^* = \{1, 2, \ldots, q-1\}$, it is computationally hard to recover a from A in polynomial amount of time t.

Definition 3 (*Computational Diffie Hellman Problem (CDHP)*)**.** Given points P, aP, $bP \epsilon G$, where $a, b \epsilon Z_q^*$, the gain of the polynomial time adversary to compute $abP \epsilon Z_q^*$ without the information of a and b is negligible.

4.1.2. Security model

Prior to proving the security of session key for proposed scheme, we illustrate RoR model.

Participants: We assume that V_i^u, HAP_j^v, and CS_k^w represent uth instance for vessel V_i, the vth instance for HAP_j, and wth instance for control station CS_k, respectively. These instance serves as the oracles in the scheme.

Accepted state : The instance V_i^u is said to be in the accepted state once the oracle receives the last expected message of the protocol. Each session is identified on the basis of session identification (sid) for V_i^u, and is produced through the concatenation of the exchanged messages by V_i^u in a particular order.

Partnering : The instances V_i^u and HAP_j^v are said to be partners, if they meet the following conditions: That is, (1) the instance V_i^u and HAP_j^v serve as mutual partners; (2) V_i^u and HAP_j^v verify the authenticity of each other for the shared session identity sid; (3) V_i^u and HAP_j^v, both are in accepted state.

Freshness : The instances V_i^u and HAP_j^v are termed as fresh once the generated session key SK_{ik} between participants is not revealed to the attacker $\mathcal{A}$.

In Canetti and Krawczyk's (CK)-attack model, $\mathcal{A}$ can manage the control of transmitted messages among the entities, besides $\mathcal{A}$ is assumed to be familiar with all publicly available parameters in the system. In addition, $\mathcal{A}$ may approach, manipulate and forge the exchanged messages in communication. The adversary may utilize the understated oracles to meet its nefarious objectives.

- $Execute(V_i^u, HAP_j^v, CS_k^w)$: Using this oracle query an attacker could model an eavesdropping threat and access the communicated messages $\{M_1, M_2, M_3, M_4, M_5, M_6\}$ in transit, exchanged among V_i, HAP_j and CS_k on public channel.
- $Reveal(V_i^u, HAP_j^v)$: The attacker may use this query to expose or uncover the established session key SK_{ik} between V_i and HAP_j participating entities.
- $Send(V_i^u, M)$: Using this oracle query, $\mathcal{A}$ may initiate active attack, and send the message M to participating instance V_i^u and gets the response message as a reply.
- $Corrupt(V_i^u)$: By employing this query, the attacker may obtain the long term secret credentials which may be stored in the stolen smart card of a legitimate V_i^u instance.
- $Test(V_i^u, HAP_j^v)$: This oracle models semantic security regarding the established session key between V_i^u and HAP_j^v. A coin c is flipped initially in this experiment, while its outcome $c \epsilon \{0,1\}$ may be closely related to attacker guess that might play a key role as output of query. In case the session key is not established, or else the instance V_i^u or HAP_j^v is not fresh, it will return null value ($\perp$). On the other hand, if $c = 1$, the instances V_i^u or HAP_j^v must return SK_{ik} to attacker. Otherwise, if c is 0, it will return any random integer to the attacker.

It is noteworthy that all of the participants including the malicious attacker may access the cryptographic one way hash function $H(\cdot)$, which is modeled as a random oracle. The following theorem is used to proceed with the analysis.

4.1.3. Formal security proof

Theorem 1. *The adversary $\mathcal{A}$ is assumed to run the contributed authenticated key agreement (AKA) model in polynomial time t. D_p is assumed to be password dictionary of size $|D_p|$ with uniform distribution. q_{sd} and q_{hs} depict the number of queries for $Send$ and $Hash$-based oracles, respectively. The range space and length for $H(\cdot)$ function may be represented by $|Hash|$ l, respectively. The advantage of the attacker for breaking the CDHP problem in at most time t is $Adv_{\mathcal{A}}^{CDHP}(t)$. Then, the gain of attacker to break the session key SK_{ik} for contributed AKA model is shown as:*

$$Adv_{\mathcal{A}}^{AKA}(t) \leq \frac{q_{hs}^2}{|Hash|} + \frac{q_{se}}{2^{l-1} \cdot |D_P|} + 2Adv_{\mathcal{A}}^{CDHP}(t) \quad (2)$$

Proof : We employ five games $G_{mi}, i = \{0 \leq i \leq 4\}$ to verify the authenticity of contributed model. We assume, SUC_{Gi} defines the success probability to guess the value of c in game G_{mi}, hence the related gain of the attacker $\mathcal{A}$ can be represented as $Pr[SUC_{Gi}]$.

Game G_{m0}: The G_{m0} being the starting game acts as the real experiment of attack by the attacker against the modeled AKA in random oracle model. The value of flipped coin c is chosen on random basis by attacker in the initialization of the experiment. As per the semantic security definition [46], we have,

$$Adv_{\mathcal{A}}^{AKA}(t) = |2.Pr[SUC_{G0}] - 1| \quad (3)$$

Game G_{m1}: The G_{m1} simulates an active attack through eavesdropping, and running $Execute(V_i^u, HAP_j^v, CS_k^w)$ oracle query. The attacker may intercept the communicated messages $M_1 = \{\alpha_{vi}, \overline{I}_{vi}\}$, $M_2 = \{t_{hj}, \alpha_{hj}, H_{hj}^1\}$, $M_3 = \{H_{vi}^1, H_{vi}^2 t_{vi}\}$, $M_4 = \{I_{hj}, C_{hj}, H_{hj}^2, H_{vi}^2, t_{hj}^2\}$, $M_5 = \{\alpha_{ck}, H_{kj}, H_{ki}, t_{ck}\}$ and $M_6 = \{\alpha_{ck}, H_{ki}, t_{ck}, t_{hj}^3\}$ during communication among the entities V_i, HAP_j and CS_k. Thereafter, the attacker runs the $Test(V_i^u, HAP_j^v)$ oracle query. After checking the output of $Test$ query, attacker might deduce whether it is able to get the legal session key SK_{ik} or some random integer. The computed session key between V_i and CS_k is $SK_{ik} = h(\alpha_{vi} \parallel \beta_{vi} \parallel \alpha_{ck} \parallel r_{vi}\alpha_{ck} \parallel K_{VC})$. If the attacker attempts to recover the session key from intercepted messages, it requires to calculate $r_{vi}\alpha_{ck}$ and $\beta_{vi} = s_{vi}\alpha_{hj}$, however for this purpose it needs access to short term secrets such as r_{vi} and s_{vi}, respectively. This must require access to long term secret K_C to compute further factors in SK_{ik}. In this scenario, the eavesdropping might not help the attacker to recover those parameters from M_1, M_2, M_3, M_4, M_5 and M_6. Thus, there are lean chances of attacker through eavesdropping attack to win the game G_{m1}. Therefore, we have

$$Pr[SUC_{G0}] = |Pr[SUC_{G1}] \quad (4)$$

Game G_{m2}: The G_{m2} simulates G_{m1} with added modeling for $H(\cdot)$ function and $Send(V_i^u, M)$ query oracle. This is also an active threat by the adversary where it attempts to make the other participant accept the fabricated message. Even the adversary may constantly issue $Hash$ queries to verify the chances of collision in the messages, however all of the exchanges messages $\{M_1, M_2, M_3, M_4, M_5, M_6\}$ are constructed using fresh timestamps, random integers, as well as identity of V_i. Thus when the attacker initiates $Send$ queries, there is no collision. Referring to the birthday paradox, we get to the following equation.

$$|Pr[SUC_{Gm2}] - Pr[SUC_G m1]| \leq \frac{q_{hs}^2}{2|hash|}. \quad (5)$$

Game G_{m3}: The simulation of $Corrupt(V_i^u)$ makes the difference for G_{m3} in comparison with G_{m2}. In the above context, the attacker may recover all secret messages $\{s_{vi}, K_{VC}\}$. If $\mathcal{A}$ attempts to guess about the identity I_{vi} of the vessel, it must require access to s_{ck} as well as k secret. In case $\mathcal{A}$ execute q_{se} times the $Corrupt$ query to guess the identity and match the s_{ck} as well as k secret, it approaches the maximum limit. The probability of $\mathcal{A}$ for wining the G_{m3} is:

$$|Pr[SUC_{Gm3}] - Pr[SUC_{Gm2}]| \leq \frac{q_{se}}{2^l|D_p|}. \tag{6}$$

Game G_{m4}: This is the last game played by adversary in which it intercepts the messages $\{M_1, M_2, M_3, M_4, M_5, M_6\}$ and attempts to calculate session key $SK_{ik} = h(\alpha_{vi} \parallel \beta_{vi} \parallel \alpha_{ck} \parallel r_{vi}\alpha_{ck} \parallel K_{VC})$ using ephemeral factors r_{vi} and K_{VC}. For computing $r_{vi}\alpha_{ck}$, it needs r_{vi}-based ephemeral secret, however even if it becomes familiar about α_{ck}, it is hard to guess the other factor r_{vi} which requires to solve CDHP problem in time t to calculate the legal session key SK_{ik} as mutually agreed between V_i and CS_k. Hence, we get

$$|Pr[SUC_{Gm4}] - Pr[SUC_{Gm3}]| \leq Adv_{\mathcal{A}}^{CDHP}(t). \tag{7}$$

Finally, the attacker models all of the oracles, and is left for guessing the value of coin c to win the game upon querying $Test(V_i^u, HAP_j)$. The probability of guessing the value of c for $Pr[SUC_{Gm4}]$ is as follows:

$$Pr[SUC_{Gm4}] = \frac{1}{2} \tag{8}$$

Using Eqs. (3), and (4), we have

$$\frac{1}{2}Adv_{\mathcal{A}}^{AKA}(t) = 2.|Pr[SUC_{Gm0}] - \frac{1}{2}| \tag{9}$$

$$= 2.|Pr[SUC_{Gm1}] - Pr[SUC_{Gm4}]| \tag{10}$$

On the basis of games (5), (6), (7) and triangular equality, we have:

$$|Pr[SUC_{Gm4}] - Pr[SUC_{Gm1}]| \leq |Pr[SUC_{Gm4}] - Pr[SUC_{Gm3}]|$$

$$+|Pr[SUC_{Gm3}] - Pr[SUC_{Gm1}]| \leq |Pr[SUC_{Gm4}] - Pr[SUC_{Gm3}]|$$

$$+|Pr[SUC_{Gm3}] - Pr[SUC_{Gm2}]| + |Pr[SUC_{Gm2}] - Pr[SUC_{Gm1}]|$$

$$\leq \frac{q_{hs}^2}{2|hash|} + \frac{q_{se}}{2^l \cdot |D_p|} + Adv_{\mathcal{A}}^{CDHP}(t) \tag{11}$$

Using Eqs. (10), (11), we get the following result:

$$Adv_{\mathcal{A}}^{AKA}(t) \leq \frac{q_{hs}^2}{2|hash|} + \frac{q_{se}}{2^{l-1} \cdot |D_p|} + Adv_{\mathcal{A}}^{CDHP}(t) \tag{12}$$

4.2. Informal analysis

This subsection presents the informal analysis of the proposed model.

4.2.1. Mutual authentication

In the proposed model, the participants V_i, HAP_j and CS_k mutually authenticate one another. That is, the V_i and HAP_j entities mutually authenticate each other on the basis of verification of β_{hj} parameter in the computed H_{hj}^1. V_i knows that the β_{vi} can only be computed by an entity having its access to its identity I_{vi} while it can only be derived from M_1 message by a legal entity having access to s_{hj} secret corresponding to public key Q_{vi}. Similarly, HAP_j authenticate V_i on account of β_{vi} parameter in the computed H_{vi}^1. Likewise, HAP_j and CS_k authenticate each other due to shared K_{HC} secret. Lastly V_i and CS_k authenticate each other on the basis of H_{Vi}^2 and H_{ki}, respectively. That is, the CS_k verify the authenticity of V_i on account of I_{vi} parameter in H_{Vi}^2, while V_i authenticates CS_k by verifying H_{ki} which comprises significant factors including β_{vi} and K_{VC}.

4.2.2. User anonymity

In the proposed model, the user remains anonymous due to the fact that its identity I_{vi} is not submitted on public channel in plaintext, rather it remains hidden in ciphertext under the cover of computed $\overline{I}_{vi}$, i.e., $\overline{I}_{vi} = I_{vi} \oplus r_{vi}Q_{hj}$. An adversary may not recover I_{vi} from $\overline{I}_{vi}$ without accessing the private secret key s_{hj} of HAP_j. At the same time, the scheme is untraceable since no single factor being submitted is identical across various sessions. That is why, no malicious entity can trace any factor that could aid the former in identifying the source of the message. Hence, our scheme is anonymous as well as untraceable.

4.2.3. Impersonation attacks

The proposed scheme is immune to V_i, HAP_j and CS_k impersonation attacks, since no adversary may initiate these impersonation attacks. In case, the attacker attempts to launch V_i impersonation attack by crafting and submitting a fake M_1 message towards HAP_j, the later may identify the possibility of this attack by verifying the H_{vi}^1 message. The HAP_j knows that β_{vi}-based challenge can only be met by a legitimate V_i. At this stage, the HAP_j may also identify the possibility of replay attack after monitoring the status of t_{vi}. Similarly, V_i may thwart HAP_j impersonation attack by checking H_{hj}^1, and it understands that β_{hj} can only be constructed by a valid HAP_j having access to s_{hj} and ultimately recover original I_{vi}. Likewise, V_i and HAP_j may counter any CS_k impersonation attack by verifying H_{ki} and H_{kj} parameters, respectively.

4.2.4. Ephemeral secrets leakage threat

The accidental disclosure of ephemeral random integers might help the adversary to compute the current and previous session keys. In proposed scheme, in case the ephemeral secret r_{vi} from V_i is exposed to the adversary, the latter will not be able to compute a mutually agreed session key for lacking the capability of computing β_{vi} parameter on account of nonavailability of critical s_{vi} secret. Similarly, it may not compute previous session keys due to adversary's lacking access to long term secret s_{vi}.

4.2.5. Man-in-the-middle attack

The proposed scheme is immune to man-in-the-middle attack (MiTM) if any adversary attempts to fabricate or replay the messages to other legal participants in order to impersonate them. As we see earlier in the mutual authentication process that all entities V_i, HAP_j and CS_k mutually authenticate one another in the same protocol. If an adversary attempts to forge the messages, fabricate or replay the contents towards a legitimate member, the latter may verify the authenticity of message and abort the message if the verification is unsuccessful. In this manner, there is least probability that the attacker may launch MiTM attack.

4.2.6. Perfect forward secrecy

The proposed scheme is compliant to the forward secrecy requirements of a protocol. In the proposed scheme, even if the private keys such as s_{vi} or s_{ck} are exposed to the adversary, the session keys SK_{ik} or SK_{ki} may not be computed by it until it has access to short term ephemeral secrets such as r_{vi} or r_{ck}, respectively.

4.2.7. Stolen verifiers attack

An adversary may compute significant details if it is able to steal verifiers information of the subscribers from the repository of the server. The proposed scheme is resistant to stolen verifiers attack as the controlling server CS_k does not maintain any verifiers in its repository corresponding to subscribers in the system.

4.2.8. De-synchronization attack

In proposed scheme, even if an adversary holds either M_5 or M_6 message on the way, it will not cause the participants V_i or CS_k de-synchronize of each other. This is because of the fact that the participants are not updating their synchronization parameters for future sessions. Instead, the proposed scheme is facilitating the participants in verification on the basis of public key as well as shared parameters. Hence, the proposed scheme is immune to de-synchronization attacks.

Table 2
Security features.

Schemes→ ↓Properties	Banerjee et al. (2019b)	Wazid et al. (2020)	Wazid et al. (2019b)	Srinivas et al. (2019)	Ever (2020)	Challa et al. (2017)	Challa et al. (2020)	Bera et al. (2020)	Our
SR_{F1}	✓	✓	✗	✓	✓	✓	✓	✓	✓
SR_{F2}	✓	✓	✓	✗	✓	✓	✓	✗	✓
SR_{F3}	✓	✓	✗	✓	✓	✗	✓	✓	✓
SR_{F4}	✓	✓	✓	✓	✗	✓	✓	✓	✓
SR_{F5}	✗	✓	✓	✓	✓	✓	✓	✓	✓
SR_{F6}	✓	✓	✓	✓	✓	✓	–	✓	✓
SR_{F7}	✓	✓	✓	✓	✓	✓	✓	✓	✓
SR_{F8}	✓	✓	✓	✓	✓	✓	✓	✓	✓
SR_{F9}	✓	✓	✓	✓	✓	✓	✓	✓	✓
SR_{F10}	✓	✓	✓	✓	✓	✓	✓	✓	✓
SR_{F11}	✓	✓	✓	✓	✓	✓	–	✓	✓
SR_{F12}	✗	✗	✓	✓	✓	✓	✓	✓	✓
SR_{F13}	✓	✓	✓	✓	✓	✓	✓	✓	✓
SR_{F14}	✓	✓	✓	✓	✓	✓	–	✓	✓

Note: SR_{F1}: Supports mutual authentication, SR_{F2}: Supports Anonymity and untraceability, SR_{F3}: User/Server impersonation attack, SR_{F4}: Offline-Password guessing attack, SR_{F5}: Stolen verifier attack, SR_{F6}: Man-in-the-middle attack, SR_{F7}: Ephemeral information leakage attack, SR_{F8}: Supports forward/backward secrecy, SR_{F9}: Replay attack, SR_{F10}: Device capture attack, SR_{F11}: Resist Denial of service attack, SR_{F12}: Protocol Correctness, SR_{F13}: Resist De-synchronization attack, SR_{F14}: Supports session key security; ✓: Resists attack/Supports security functionality, ✗: Do not resist attack or support security functionality.

Table 3
Computational costs.

	V_i	CS_k	HAP_j	RT (ms)
Banerjee et al. (2019b)	$1T_{fe} + 12T_{hf} + 3T_{sed}$	$19T_{hf}$	$10T_{sed}$	≈2.3571
Wazid et al. (2020)	$1T_{fe} + 17T_{hf}$	$8T_{hf}$	$9T_{hf}$	≈2.3042
Wazid et al. (2019b)	$16T_{hf} + 1T_{fe}$	$8T_{hf}$	$7T_{hf}$	≈2.2973
Srinivas et al. (2019)	$14T_h$	$14T_{hf}$	$30T_{hf} + 1T_{fe}$	≈2.3594
Ever (2020)	$5T_{hf} + 2T_b$	$3T_{hf} + 2T_b$	$9T_{hf} + 2T_b + 1T_{ecm}$	≈34.9051
Challa et al. (2017)	$5T_{hf} + 1T_{fe} + 5T_{ecm}$	$4T_{hf} + 5T_{ecm}$	$3T_{hf} + 4T_{ecm}$	≈33.4176
Challa et al. (2020)	$10T_{hf} + T_{ecm} + T_{fe}$	$5T_{hf} + T_{ecm}$	$5T_{hf}$	≈6.724
Bera et al. (2020)	$4T_{ecm} + 2T_{eca} + 4T_{hf}$	–	$4T_{ecm} + 2T_{eca} + 4T_{hf}$	≈17.9416
Our	$5T_{hf} + 3T_{ecm}$	$5T_{hf} + 2T_{ecm} + T_{sym}$	$3T_{hf} + 3T_{ecm} + T_{sym}$	≈17.8471

Note: RT (ms): Running Time in milli-seconds.

4.2.9. Denial-of-Service (DoS) attack

The proposed scheme is resistant of DoS attack since the entity CS_k does not require any access to secondary storage during the session. On the other hand, the attacker could have exploit this limitation to initiate fabricated requests towards CS_k and overburden it to affect its routine functionality. Thus, our scheme can resist DoS threats.

5. Performance evaluation

This section presents the performance evaluation analysis of various schemes (Banerjee et al., 2019b; Bera et al., 2020; Challa et al., 2017, 2020; Wazid et al., 2020, 2019b; Ever, 2020; Srinivas et al., 2019) against the proposed scheme. In order to evaluate the performance analysis in terms of cryptographic operations, we represent the execution time of hash function as T_{hf}, elliptic curve (EC) based point multiplication operation as T_{ecm}, EC-based point addition operation as T_{eca}, symmetric operation as T_{sym} and bilinear operation as T_b. We base our results from the experiment conducted in Kilinc and Yanik (2013) in which the operations T_{hf}, T_{sym}, T_{ecm}, T_{eca}, T_b, and T_{fe} take 0.0023 ms, 0.0046 ms, 2.226 ms, 0.0288 ms, 5.811 ms, and 2.226 ms, respectively. It is obvious from Table 2 that (Banerjee et al., 2019b) may not resist stolen-verifier attack, while the protocol bears many correctness problems (Chaudhry et al., 2021). The scheme (Wazid et al., 2019b) has few security limitations with protocol flaws according to Chaudhry et al. (2021). The scheme (Wazid et al., 2020) does not support mutual authentication for the participants, and is vulnerable to user impersonation attack. The schemes (Srinivas et al., 2019; Bera et al., 2020) do not support anonymity for the user. The schemes (Ever, 2020; Challa et al., 2017) are prone to offline password guessing attack and user impersonation attack, respectively. The Table 3 shows the computational costs of various schemes including symmetric as well as asymmetric cryptography schemes. It is evident from the table that the schemes with symmetric operations are low cost schemes. These schemes such as (Banerjee et al., 2019b; Wazid et al., 2020, 2019b; Srinivas et al., 2019) take computational cost of 2.35, 2.30, 2.29, 2.35 ms, respectively. However these are prone to security vulnerabilities such as lacking perfect forward secrecy along with other problems. The schemes (Bera et al., 2020; Challa et al., 2017, 2020; Ever, 2020) bear costly elliptic curve and bilinear operations along with security gains yet with limitations. The proposed scheme takes the computational cost of 17.84 ms with most of the security features as compared to the other schemes in comparison (Banerjee et al., 2019b; Bera et al., 2020; Challa et al., 2017, 2020; Wazid et al., 2020, 2019b; Ever, 2020; Srinivas et al., 2019). Moreover, it bears less cost than (Bera et al., 2020; Ever, 2020; Challa et al., 2017). The Table 4 depicts the communicational costs of the comparative schemes (Banerjee et al., 2019b; Bera et al., 2020; Challa et al., 2017, 2020; Wazid et al., 2020, 2019b; Ever, 2020; Srinivas et al., 2019) as well as proposed scheme. The communication cost is computed with an assumption of 160-bit for communicating the message of SHA-1 hash function parameter or identity, 32-bit for time stamp, and 320-bits for transmitting elliptic curve based multiplication factors. The proposed scheme has a little bit higher communication cost comparatively, yet it bears more security features with comparable computational cost as depicted from the formal analysis as well as performance evaluation. Moreover, the proposed scheme bears 17% more security features in comparison with contemporary schemes.

6. Conclusion

Maritime Communication Network (MCN) faces numerous security and privacy threats, including vessel tracking, unauthorized data access, and message modification. Many authentication schemes have been proposed recently, as discussed in the literature review of this

Table 4
Communication cost analysis.

Scheme.→	Banerjee et al. (2019b)	Wazid et al. (2020)	Wazid et al. (2019b)	Srinivas et al. (2019)	Ever (2020)	Challa et al. (2017)	Challa et al. (2020)	Bera et al. (2020)	Our
Bits Exch.	2304	1696	1696	1536	1920	2528	1536	1696	2880

article; nevertheless, none of them are fully secure against a variety of attacks. Keeping these vulnerabilities in mind, we proposed a lightweight authentication scheme to address these vulnerabilities. To validate the security characteristics, formal security assessment methods are utilized, i.e., Random Oracle Model (ROM). Also, a detailed comparison study is conducted to assess the feasibility of the proposed scheme. The results from both the studies reveal that the proposed scheme outperforms its counterpart schemes in terms of security toughness and has a better security-to-efficiency tradeoff. In future, we will emphasize to come up with even more lightweight symmetric solutions for MCN.

CRediT authorship contribution statement

Muhammad Asghar Khan: Writing – original draft, System models, Literature review. **Bander A. Alzahrani:** Writing – revised draft, Implementation. **Ahmed Barnawi:** Validation, Formal analysis. **Abdullah Al-Barakati:** Writing – review & editing, Informal analysis. **Azeem Irshad:** Performance analysis, Validation, Formal and informal security proof. **Shehzad Ashraf Chaudhry:** Conceptualization, Methodology, Software, Supervision.

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.

Acknowledgments

This project was funded by the Deanship of Scientific and Research (DSR) at King Abdulaziz University, Jeddah, under grant no (RG-3-611-41). The authors, therefore, acknowledge with thanks DSR technical and financial support.

References

Ali, Z., Chaudhry, S.A., Mahmood, K., Garg, S., Lv, Z., Z., Y.B.Z., 2021. A clogging resistant secure authentication scheme for fog computing services. Comput. Netw. 185, 10773.

Arteaga, S.P., Hernández, L.A.M., Pérez, G.S., Orozco, A.L.S., Villalba, L.J.G., 2019. Analysis of the GPS spoofing vulnerability in the drone 3Dr solo. IEEE Access 7, 51782–51789.

Banerjee, S., Chunka, C., Sen, S., Goswami, R.S., 2019a. An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. Wirel. Pers. Commun. 107 (1), 243–270.

Banerjee, S., Odelu, V., Das, A.K., Srinivas, J., Kumar, N., Chattopadhyay, S., Choo, K.-K.R., 2019b. A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment. IEEE Internet Things J. 6 (5), 8739–8752.

Bera, B., Chattaraj, D., Das, A.K., 2020. Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment. Comput. Commun. 153, 229–249.

Canetti, R., Krawczyk, H., 2002. Universally composable notions of key exchange and secure channels. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 337–351.

Challa, S., Das, A.K., Gope, P., Kumar, N., Wu, F., Vasilakos, A.V., 2020. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. Future Gener. Comput. Syst. 108, 1267–1286.

Challa, S., Wazid, M., Das, A.K., Kumar, N., Reddy, A.G., Yoon, E.-J., Yoo, K.-Y., 2017. Secure signature-based authenticated key establishment scheme for future IoT applications. Ieee Access 5, 3028–3043.

Chaudhry, S.A., Irshad, A., Yahya, K., Kumar, N., Alazab, M., Zikria, Y.B., 2021. Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment. ACM Trans. Internet Technol. (TOIT) 21 (3), 1–19.

Chaudhry, S.A., Shon, T., Al-Turjman, F., Alsharif, M.H., 2020. Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. Comput. Commun. 53, 527–537.

Das, A.K., Wazid, M., Kumar, N., Vasilakos, A.V., Rodrigues, J.J.P.C., 2018. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. IEEE Internet Things J. 5 (6), 4900–4913.

Das, A.K., Wazid, M., Yannam, A.R., Rodrigues, J.J.P.C., Park, Y., 2019. Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access 7, 55382–55397.

Dolev, D., Yao, A., 1983. On the security of public key protocols. IEEE Trans. Inf. 29, 2.

Ever, Y., 2020. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. Comput. Commun. 155, 143–149.

Farash, M.S., Turkanovi'c, M., Kumari, S., H"olbl, M., 2016. 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.

Guan, S., Wang, J., Jiang, C., Duan, R., Ren, Y., Quek, T.Q.S., 2021. MagicNet: The maritime giant cellular network. IEEE Commun. Mag 59 (3), 117–123.

Guo, Y., Wu, M., Tang, K., Tie, J., Li, X., 2019. Covert spoofing algorithm of UAV based on GPS/INS-Integrated navigation. IEEE Trans. Veh. Technol. 68 (7), 6557–6564.

Huo, Y., Dong, X., Beatty, S., 2020. Cellular communications in ocean waves for maritime internet of things. IEEE Internet Things J. 7 (10), 9965–9979. http://dx.doi.org/10.1109/JIOT.2020.2988634.

Hussain, S., Chaudhry, S.A., 2019. Comments on "biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment,". IEEE Internet Things J. 6 (6), 10936–10940.

Hussain, S., Chaudhry, S.A., Alomari, O.A., Alsharif, M.H., Khan, M.K., Kumar, N., 2021. "Amassing the security: An ECC-based authentication scheme for internet of drones," IEEE syst. J. Early Access, Mar 1.

Khan, M.A., Ullah, I., Kumar, N., Oubbati, O.S., Qureshi, I.M., Noor, F., Ullah Khanzada, F., 2021. An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks. IEEE Transactions on Vehicular Technology 70 (5), 4839–4851. http://dx.doi.org/10.1109/TVT.2021.3055895.

Kilinc, H.H., Yanik, T., 2013. A survey of SIP authentication and key agreement schemes. IEEE Commun. Surv. Tutor. 16 (2), 1005–1023.

Liu, J., Shi, Y., Fadlullah, Z.M., Kato, N., 2018. Space-air-ground integrated network: A survey. IEEE Commun. Surveys Tuts 20 (4), 2714–2741.

Malani, S., Srinivas, J., Das, A.K., Srinathan, K., Jo., M., 2019. Certificatebased anonymous device access control scheme for IoT environment. IEEE Internet Things J. 6, 6.

Motlagh, N.H., Taleb, T., Arouk, O., 2016. Low-altitude unmannedaerial vehicles-based internet of things services: Comprehensive surveyand future perspectives. IEEE Internet Things J. 3 (6), 899–922.

Odelu, V., Das, A.K., Choo, K.R., Kumar, N., Park, Y., 2017. Efficient and secure time-key based single sign-on authentication for mobile devices. IEEE Access 5, 27707–27721.

Srinivas, J., Das, A.K., Kumar, N., Rodrigues, J.J.P.C., 2019. Tcalas: temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. IEEE Transactions on Vehicular Technology 68 (7), 6903–6916. http://dx.doi.org/10.1109/TVT.2019.2911672.

Turkanovi/'c, M., Brumen, B., H"olbl, M., 2014. 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.

Wang, H., Osen, O.L., Li, G., Li, W., Dai, H., Zeng, W., 2015. Big data and industrial internet of things for the maritime industry in Northwestern Norway. In: Macao, C. (Ed.), Proc. IEEE Region 10 Conf. pp. 1–5.

Wazid, M., Das, A.K., Bhat, V., Vasilakos, A.V., 2020. LAM-cIoT: Lightweight authentication mechanism in cloud-based IoT environment. J. Netw. Comput. Appl. 150, 102496.

Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V., 2019a. Design of secure key management and user authentication scheme for fog computing services. Future Gener. Comput. Syst. 91, 475.

Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V., Rodrigues, J.J.P.C., 2019b. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drone's deployment. IEEE Internet Things J. 6 (2), 3572–3584.

Wei, T., Feng, W., Chen, Y., Wang, C.-X., Ge, N., Lu, J., 2021. Hybrid satellite-terrestrial communication networks for the maritime internet of things: Key technologies, opportunities, and challenges. IEEE Internet Things J. 8, 8910–8934.

Xia, T., Wang, M.M., Zhang, J., Wang, L., 2020. Maritime internet of things: Challenges and solutions. IEEE Wirel. Commun. 27 (2), 188–196.

Zhang, J., Wang, M.M., Xia, T., Wang, L., 2020. Maritime IoT: An architectural and radio spectrum perspective. IEEE Access 8, 93109–93122.