A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System

Shehzad Ashraf Chaudhry, Azeem Irshad, Muhammad Asghar Khan, Sajjad Ahmad Khan, Summera Nosheen, *Member, IEEE*, Ahmad Ali AlZubi, and Yousaf Bin Zikria, *Senior Member, IEEE*

***Abstract*— The Sixth-Generation (6G) mobile network has the potential to provide not only traditional communication services but also additional processing, caching, sensing, and control capabilities to a massive number of Internet of Things (IoT) devices. Meanwhile, a 6G mobile network may provide global coverage and diverse quality-of-service provisioning to the Maritime Transportation System (MTS) when enabled through satellite systems. Although modern MTS has gained significant benefits from Internet of Things (IoT) and 6G technologies, threats and challenges in terms of security and privacy have also been grown substantially. Tracking the location of vessels, GPS spoofing, unauthorized access to data, and message tampering are some of the potential security and privacy vulnerabilities in the 6G-IoT enabled MTS. In this article, we propose a lightweight authentication protocol for a 6G-IoT enabled maritime transportation system to efficiently assist and ensure the security and privacy of maritime transportation systems. To validate the security characteristics, formal security assessment methods are utilized, i.e., Real-Or-Random (ROR) oracle model. The findings of the security analysis show that the proposed scheme is more secure than the existing schemes.**

***Index Terms*— Device access control, maritime transportation system, device impersonation, forged message, IoT access.**

I. Introduction

THE rapid development of the Internet of Things (IoT) devices, sensors, and beyond 5G technologies led to a new era in the maritime transportation industry and research. Meanwhile, satellite operators seek cost-effective communication services over the oceans by employing a multi-layer aerial component, including a High Altitude Platform System (HAPS) and small drones. As a result, executives in the marine industry are increasingly adopting IoT applications with caution and attention to achieve returns on investment. Modern Maritime Transportation Systems (MTS)have significantly benefited from IoT, 6G, and satellite technologies, which may improve the operational performance of the maritime transportation systems. Additionally, the availability of low-cost, high-performance drones has made the deployment of drone base stations feasible [1]–[4], which HAPS facilitates, a critical vertical component of the 5G and beyond ecosystem [5]. A 6G-IoT equipped MTS can easily handle navigation and real-time vessel tracking, vessel-to-vessel and vessel-to-shore information exchange, cargo scheduling and management, and vessel safety and operations [6]–[8]. The 6G mobile network is capable of supporting a wide range of current and future MTS applications, including autonomous services and emerging trends. It will be able to deliver network speeds of over 1Tbps with a latency of less than 1ms and enable autonomous vessel movement up to 1000 km/h. It also provides capacity expansion strategies to address the issue of ubiquitous connectivity, even in exceptional or emergencies when infrastructure density, bandwidth, and traffic patterns may vary. However, most of these systems were designed before the widespread threats of cyber-attacks that have become common due to the extensive deployment of IoT devices with wireless connections. As a result, ensuring the security and privacy of data generated from a large number of IoT devices positioned on the vessels is important. The marine industry, for example, has been subjected to several cyber-attacks [9]. GPS jamming, cargo system manipulation, and ransomware attacks are among the recent cyber security concerns in this sector. Intruders may cause uncertainty throughout the system and leak sensitive data if there are no countermeasures to ensure data security and privacy features. For example, Global Positioning System (GPS) spoofing [10]–[14], in which an adversary uses GPS signals, is a serious security issue affecting the privacy of 6G-IoT enabled MTS. In this attack, an adversary sends fraudulent GPS signals to a targeted vessel that is slightly stronger than actual GPS signals to mislead 6G-IoT equipped vessels from their original destination and steer them to the adversary's chosen location. As a consequence, advanced security measures for 6G-IoT MTS have become one of the most critical requirements.

Manuscript received 13 September 2021; revised 11 November 2021; accepted 7 December 2021. Date of publication 22 December 2021; date of current version 8 February 2023. This work was supported by King Saud University, Riyadh, Saudi Arabia, under Researchers Supporting Project RSP-2021/395. The Associate Editor for this article was A. K. Bashir. *(Corresponding authors: Summera Nosheen; Yousaf Bin Zikria.)*

Shehzad Ashraf Chaudhry is with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 İstanbul, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Azeem Irshad is with the Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan (e-mail: irshadazeem2@gmail.com).

Muhammad Asghar Khan is with the Department of Electrical Engineering, Hamdard University, Islamabad 44000, Pakistan (e-mail: khayyam2302@gmail.com).

Sajjad Ahmad Khan is with the Electronics and Communication Engineering Department, Faculty of Electrical and Electronics Engineering, Istanbul Technical University (ITU), 34469 İstanbul, Turkey, and also with the Department of Software Engineering, Istanbul Gelisim University, 34310 İstanbul, Turkey (e-mail: skhan@itu.edu.tr).

Summera Nosheen is with the School of Electrical Engineering and Computing, The University of Newcastle, University Dr, Callaghan NSW 2308, Australia (e-mail: summera.nosheen@uon.edu.au).

Ahmad Ali AlZubi is with the Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia (e-mail: aalzubi@ksu.edu.sa).

Yousaf Bin Zikria is with the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan-si 38541, South Korea (e-mail: yousafbinzikria@ynu.ac.kr).

Digital Object Identifier 10.1109/TITS.2021.3134643

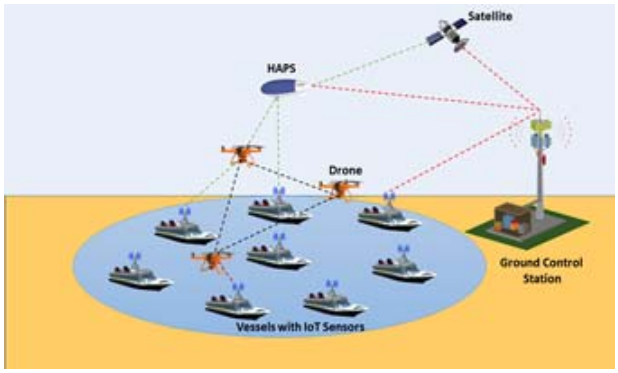

Fig. 1. Sample architecture for 6G-IoT enabled MTS.

Unfortunately, these efforts will not be sufficient to resolve the communication problems between vessels, HAPS, and ground control stations (GCS). Drones equipped with communication equipment may be utilized to address this problem and may be used to perform various tasks, such as low-altitude surveillance and communication assistance. The advantages of a drone-supported 6G-IoT enabled MTS over traditional MTS are significant. To begin with, the signal loss may be significantly reduced because the drone may move closer to vessels than fixed base stations. Second, the speed and transmission power of drones may change based on the mobility of the vessels. Finally, the efficiency of drone-to-vessel connections is typically higher than terrestrial connectivity because of line-of-sight contact [15]. Drones are thus seen as a convincing option for providing communication and solutions for 6G-IoT enabled MTS because of their ease of access feature.

As illustrated in Fig. 1, the future MTS will incorporate satellites that help achieve global coverage for maritime communications and drones that may act as a relay. HAPS, which are often installed above the stratospheric layer, can provide more coverage/relay and collaborate with satellites to build more dependable maritime networks, especially when satellite communications are disrupted by bad weather. The vessels are comprised of a variety of IoT sensors that help in operations. They are also committed to gathering and disseminating event-driven messaging. Finally, the Ground Control Station (GCS) maintains control over the whole transportation system. Some prominent traits of this research study are given as follows:

- We develop and present a lightweight and secure message authentication protocol for maritime transport system (LSMP-MTS), comprised of drones, satellites, and a High-Altitude Platform System (HAPS) that uses IoT and 6G wireless technologies.
- LSMP-MTS uses lightweight primitives of symmetric cryptography, including XoR and hash operations, in addition to the symmetric block cryptography, which affirm the performance efficiency of the proposed LSMP-MTS.
- The proposed LSMP-MTS provides authentication and commutation of a shared key for safe future communication among the MTS entities. It also protects vessel privacy and anonymity.
- The commuted shared key among entities of the proposed LSMP-MTS contains the short-term parameters (r_{vi} and r_{ck}) contributed by each of the vessel V_i and CS_k as well as long-term vessel related secret parameter $X_i = h(K_C||VID_i)$. Therefore, proposed scheme provides perfect forward secrecy and privacy/confidentiality of the session key SK_{cv}.

A. 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 I-B. We go through system models in Section II, which also includes network and threat models. In Section III, the proposed model and algorithm are defined. Section IV, on the other hand, provides the proposed scheme's security analysis. In addition, we discuss performance analysis in Section V. The conclusion is presented in Section VI.

B. Related Work

In a 6G-IoT enabled MTS, secured communication plays an important role because the communication is usually taking place in an open and insecure wireless channel. Authenticity, anonymity, and data integrity are the major problems that need to be addressed. As a result, an effective authentication scheme must be implemented for a 6G-IoT enabled MTS environment to provide a defined measurable against intrusions. To address this concern, Tian *et al.* [16] presented a certificate-oriented authenticated key agreement scheme for the Internet of Drones (IoD) that included edge computing functionality. In the proposed scheme, the authors employed the RSA technique. Under the CK-adversary model, the scheme failed to protect against Ephemeral Secret Leakage (ESL) attacks. Rodrigues *et al.* [17] proposed an authentication system for drone communication networks using an Elliptic Curve Cryptography (ECC) technique. When utilizing the CK-attack model with blockchain-based security, nonetheless, the protocol is prone to ESL attacks. Furthermore, the device addition phase is not supported by the proposed scheme. Ever [18] and Nikooghadam *et al.* [19] proposed a similar kind of scheme, which is ECC-based authentication for safe UAV deployment. On the other hand, neither approach succeeds in maintaining anonymity and unreliability. Zhang *et al.* [20] presented an anonymous authentication and key agreement scheme for 5G/B5G vehicle ad-hoc networks.

The scheme is shown to be resilient against well-known threats using ROR model. Rajakumar *et al.* [21] also proposed a scheme to provide key agreement and mutual authentication in LTE networks. For the IoD environment, Wazid *et al.* [22] presented a new lightweight key agreement protocol that employed bitwise XOR and collision resistant one-way hash algorithms. The scheme, however, does not provide a session key agreement. Zhang *et al.* [23] presented a better alternative to address this shortcoming. However, the presented scheme additionally demands the use of a control server. Srinivas *et al.* [24] presented a user authentication protocol for drones that employs several authentication factors, including mobile device, biometric, and password. The proposed

scheme uses temporary credentials to preserve user privacy while also preventing unauthorized access to drones. The proposed scheme also depended largely on trustworthy ground stations serving as gateways and remote-control centers. Turkanovic *et al.* [25] are subjected to the same criticisms. Farash *et al.* [26] shown that Turkanovic *et al.* [25] scheme is prone to several cryptographic attacks. After then, Farash *et al.* presented a better technique for securing three-party settings. Al-Turjman *et al.* [27] introduced a seamless key agreement structure in an IoT-based cloud-centric network. The proposed protocol is susceptible to DoS threat, offline-password guessing, and key impersonation threat. Hussain *et al.* [28] proposed secure and lightweight user access, which showed that Wazid *et al.* [22] user access to drone scheme is subjected to various attacks, including stolen verifier and traceability attacks. Chaudhry *et al.* [29] identified flaws by evaluating a recent hash operations-based authentication method for cloud-oriented IoT devices with a misinterpreted privacy/efficiency tradeoff due to an apparent design error that is common in many other protocols. The authors also demonstrated that the Wazid *et al.* technique could not offer authenticated key agreement on a mutual basis between the user and sensor node when there are several registered users. Similarly, Ali *et al.* [30] proposed a secure fog computing authentication scheme that is immune to clogging attacks. However, their scheme authentication procedure necessitates the use of a cloud server. Ali *et al.* [31] proposed a wireless healthcare sensor network authentication scheme with access control. Their scheme does not include a multi-server architecture. With the shortcomings mentioned above in mind, creating a newer authentication scheme has become critical. The protocol must be capable of coping with a variety of security and privacy challenges unmet by existing schemes. Our proposed scheme intends to provide a comprehensive solution that meets all security requirements.

II. System Models

To describe the operation and implementation of the proposed scheme, details about the network and threat model are as follows:

A. Network Model

The proposed network model, as illustrated in Fig. 1, is made up of five types of entities: vessels with IoT devices, drones, High Altitude Platform System (HAPS), satellites, and Control Station (CS). The vessels are outfitted with a wide range of sensors and IoT devices that help make better decisions for operations like route and delivery planning, cargo scheduling and management, and weather forecasting. These sensors and IoT devices are primarily dedicated to collecting and disseminating event-driven messages related to MTS. Alongside the designated vessel, a drone equipped with a camera, an Inertial Measurement Unit (IMU), sensors, and a Global Positioning System (GPS) unit may fly. Because of their agile maneuverability, drones are considered an efficient entity for achieving dynamic and flexible coverage for MTS. Satellites, on the other hand, aid in the attainment of worldwide maritime communications coverage. Unlike terrestrial communication systems, Satellite services rely on geostationary satellites to broadcast and receive signals in areas outside the range of shore stations. Additionally, HAPS provides greater coverage/relay and interacts with satellites, allowing for more reliable maritime communication networks, significantly when satellite communications are disrupted by bad weather. HAPS may use 6G, and there is no need for extra equipment on the drones or the vessels.

TABLE I
Notations Guide

Symbols	Representations
V_i, CS_k, HAP_j	Vessel, control station, HAP
VID_i, HID_j, CID_k	ID's of V_i, HAP_j, CS_k
K_C	Secret key of CS_k
K_{HC}	Shared key among CS_k and HAP_j
t_x, r_x	Timestamp and random number of x
PID_i	Pseudo identity of V_i
$H(a), \|\|$	Hash of a and Concatenation
$E_k(Z)$	Symmetric encryption of Z using key k
t_p	Present timestamp recorded at respective entity

B. Threat Model

According to reports, the extensively used "Canetti and Krawczyk's adversary model (CK-adversary model)" [32] is a de facto standard for modeling authentication schemes, which is adopted in this paper and is an extension to Dolev-Yao (DY) model. The DY model involves insecure public channel communication, and mistrust among the participants [33]. Hence, a malicious adversary may easily intervene and approach the contents of the communications. According to the CK-attack model, the adversary may also compromise the session states, secret parameters, and other credentials.

III. Proposed LSMP-MTS

This section explains the Lightweight and Secure Message Exchange Protocol for Maritime Transportation System(LSMP-MTS). The key notations and definitions used in the proposed LSMP-MTS scheme are listed in Table I. Initialization, HAPS registration, and vessel registration are the three phases that constitute our proposed scheme. The following are descriptions of each phase.

A. LSMP-MTS: Initialization

The Control Station (CS) selects it's secret key K_C, own identity ID_c a one way hash function $H() : \{0, 1\}^* \rightarrow \{0, 1\}^l$ and a symmetric encryption/decryption function $X = E_k(Y)$.

B. LSMP-MTS: HAP Registration

During this phase, Control Station (CS) registers all High Altitude Platform System (HAPs) by assigning a unique identity HID_j and a shared key $K_{HC} = h(HID_j||K_C||CN)$, where CN is a counter and is initialized by 0, CN is incremented whenever the shared key needs to be updated or the HAP re-registers with the system. The control station stores $\{HID_j, CN\}$ in it's database.

$\mathcal{V}_i$	$\mathcal{HAP}_j$	$\mathcal{CS}_k$
Generate t_{vi} and r_{vi}		
$P_{vi} = h(X_i \| \| VID_i \| \| t_{vi} \| \| r_{vi})$	Check $\|t_p - t_{vi}\| \leq \Delta T$	
$Q_{vi} = r_{vi} \oplus Y_i$	Generate t_{hj} and r_{hj}	Check $\|t_p - t_{hj}\| \leq \Delta T$
$\xrightarrow{M_{vhc}=\{PID_i, P_{vi}, Q_{vi}, t_{vi}\}}$	$P_{hj} = E_{K_{HC}}(HID_j, r_{hj}, t_{hj})$	$K_{HC} = h(HID_j \| \| K_C \| \| CN)$
	$\xrightarrow{M_{hc}=\{HID_j, M_{vhc}, P_{hj}, t_{hj}\}}$	$(HID_j, r_{hj}, t_{hj}) = D_{K_{HC}}(P_{hj})$
		$t'_{hj} \stackrel{?}{=} t_{hj}$
		$(VID_i, r_0) = D_{K_C}(PID_i)$
		$X_i = h(K_C \| \| VID_i)$
		$Y_i = h(VID_i \| \| K_C \| \| CID_k)$
		$r_{vi} = Y_i \oplus Q_{vi}$
		$P_{vi} \stackrel{?}{=} h(X_i \| \| VID_i \| \| t_{vi} \| \| r_{vi})$
		Generate r_{ck}, t_{ck} and compute
		$SK_{cv} = h(r_{vi} \| \| r_{ck} \| \| X_i \| \| VID_i)$
		$PID_i^{nw} = E_{K_C}(VID_i, r_{ck})$
		$R_{CH} = E_{K_{HC}}(r_{hj}, PID_i^{nw})$
	Check $\|t_p - t_{ck}\| \leq \Delta T$	$R_{CV} = E_{X_i}(r_{ck}, PID_i^{nw}, t_{ck})$
Check $\|t_p - t_{hj}^2\| \leq \Delta T$	$(r_{hj}, PID_i^{nw}) = E_{K_{HC}}(R_{CH})$	$V_{CH} = h(r_{hj} \| \| PID_i^{nw} \| \| t_{ck})$
$(r_{ck}, PID_i^{nw}, t_{ck}) = D_{X_i}(R_{CV})$	$V_{CH} \stackrel{?}{=} h(r_{hj} \| \| PID_i^{nw} \| \| t_{ck})$	$V_{CV} = h(SK_{cv} \| \| r_{vi} \| \| r_{ck} \| \| PID_i^{nw})$
$V_{CV} \stackrel{?}{=} h(SK_{cv} \| \| r_{vi} \| \| r_{ck} \| \| PID_i^{nw})$	Store PID_i^{nw}, Generate t_{hj}^2	$\xleftarrow{M_{chv}=\{R_{CH}, R_{CV}, V_{CH}, V_{CV}, t_{ck}\}}$
$PID_i = PID_i^{nw}$	$\xleftarrow{M_{hv}=\{R_{CV}, V_{CV}, t_{hj}^2\}}$	

Fig. 2. Proposed LSMP-MTS.

C. LSMP-MTS: Vessel Registration

During this phase, Control Station registers all vessels $\{V_i : I = 1, 2 \ldots n\}$ by assigning a unique identity VID_i. Moreover, CS computes $X_i = h(K_C \| \| VID_i)$, $Y_i = h(VID_i \| \| K_C \| \| CID_k)$ and $PID_{vi} = E_{K_C}(VID_i, r_0)$ and sends $\{VID_i, PID_i, X_i, Y_i\}$ to V_i, which in turn stores these parameters in it's memory. The CS stores VID_i, PID_i, X_i and Y_i in V_i's memory. Further the VS stores VID_i in it's own memory.

D. LSMP-MTS: Mutual Authentication

The steps to conclude this phase are depicted in Fig. 2 and are explained as follows:

- During this phase, V_i generate timestamp t_{vi} and a random integer r_{vi}. Then it computes $P_{vi} = h(X_i \| \| VID_i \| \| t_{vi} \| \| r_{vi})$, $Q_{vi} = r_{vi} \oplus Y_i$. Then V_i submits $M_{vhc} = \{PID_i, P_{vi}, Q_{vi}, t_{vi}\}$ to HAP_j.
- After receiving the M_{vhc} message, the HAP_j checks the freshness of timestamp t_{vi} by matching against the threshold ΔT. It aborts if t_{vi} is not fresh. Or else, it generates t_{hj} and r_{hj}. Next it computes $P_{hj} = E_{K_{HC}}(HID_j, r_{hj}, t'_{hj})$, and submits $M_{hc} = \{HID_j, M_{vhc}, P_{hj}, t_{hj}\}$ to CS_k.
- Upon the receipt of M_{vhc} message, the CS_k monitors the freshness of t_{hj}. It terminates the session if t_{hj} is not fresh. Or else, it calculates $K_{HC} = h(HID_j \| \| KC \| \| CN)$ and $(HID_j, r_{hj}, t'_{hj}) = D_{K_{HC}}(P_{hj})$. Next, it verifies the equality for $t'_{hj}? = t_{hj}$. It aborts if it is not matched. Otherwise, computes: $(VID_i, r_0) = D_{KC}(PID_i)$, $X_i = h(KC \| \| VID_i)$, $Y_i = h(VID_i \| \| KC \| \| CID_k)$, $r_{vi} = Y_i \oplus Q_{vi}$, $P_{vi}? = h(X_i \| \| VID_i \| \| t_{vi} \| \| r_{vi})$. Next, it generates r_{ck} random integer and fresh timestamp t_{ck}. Further, it computes $SK_{cv} = h(r_{vi} \| \| r_{ck} \| \| X_i \| \| VID_i)$, $PID_i^{nw} = E_{KC}(VID_i, r_{ck})$, $R_{CH} = E_{K_{HC}}(r_{hj}, PID_i^{nw})$, $R_{CV} = E_{X_i}(PID_i^{nw}, t_{ck})$, $V_{CH} = h(r_{hj} \| \| PID_i^{nw} \| \| t_{ck})$ and $V_{CV} = h(SK_{cv} \| \| r_{vi} \| \| r_{ck} \| \| PID_i^{nw})$. Finally, it sends the message $M_{chv} = \{R_{CH}, R_{CV}, V_{CH}, V_{CV}, t_{ck}\}$ to HAP_j.
- After receiving M_{vhc} message, the HAP_j checks the freshness of t_{ck}. It aborts the session if t_{ck} is not fresh. Otherwise, computes $(r_{hj}, PID_i^{nw}) = E_{K_{HC}}(R_{CH})$. Then it verifies the equality for $V_{CH}? = h(r_{hj} \| \| PID_i^{nw} \| \| t_{ck})$. It terminates the session on the mismatch of equality. Otherwise, stores PID_i^{nw} in its repository, generates timestamp t_{hj}^2 and submits $M_{hv} = \{R_{CV}, V_{CV}, t_{hj}^2\}$ to V_i.
- The V_i, after receiving M_{hv}, checks the freshness of t_{hj}^2. If it is valid, it further computes $(r_{ck}, PID_i^{nw}, t_{ck}) = D_{X_i}(R_{CV})$ and $SK_{cv} = h(r_{vi} \| \| r_{ck} \| \| X_i \| \| VID_i)$. Then it verifies the equality for $V_{CV}? = h(SK_{cv} \| \| r_{vi} \| \| r_{ck} \| \| PID_i^{nw})$. It terminates the session if equation is not matched. Otherwise, replaces PID_i with PID_i^{nw} in its repository.

E. Communication Phase

Once the session key is mutually agreed between the V_i and CS_k, the same participants can establish the communication by employing the steps shown in Fig. 3 and explained as follows:

- First the V_i generates a random integer t_{vi} and compute $(v_i = E_{SK_{cv}}(m_{vi}, t_{vi})$ and submits $\{PID_i, C_{vi}, t_{vi}\}$ to HAP_j.
- The HAP_j after verifying the PID_i in its' database, appends its identity to the same message. Then, it submits $\{PID_i, C_{vi}, t_{vi}, HID_j\}$ to CS_k.
- The CS_k verifies the freshness of timestamp t_{vi}. If this check fails, it will terminate the communication session. Otherwise, it computes $(VID_i, r_i) = D_{KC}(PID_i)$, $(m_{vi}, t'_{vi}) = D_{SK_{cv}}(C_{vi})$. It endorses the message m_{vi}, if the timestamp t_{vi} is matched against the decrypted t'_{vi}. Next, it further generate a random number t_{ck}, computes $C_{ck} = E_{SK_{cv}}(m_{ck}, t_{ck})$, and submits the message $\{CID_k, C_{ck}\}$ towards HAP_j.
- The HAP_j appends its identity HID_j into this message and forwards to V_i.

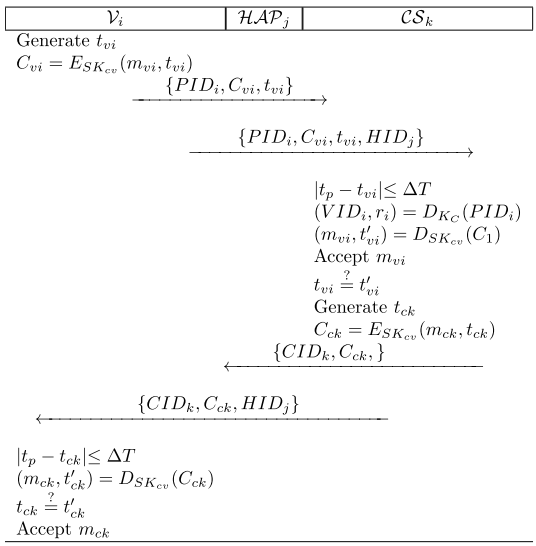

Fig. 3. Communication phase.

- The V_i, ultimately checks the freshness of timestamp t_{ck}, and computes $(m_{ck}, t'_{ck}) = D_{SK_{cv}}(C_{ck})$. Next, it compares t_{ck} against the recovered t'_{ck} and accept m_{ck}.

IV. Security Analysis

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

A. Formal Security Analysis

This section depicts the security analysis of the contributed model formally under the principles of the universally accepted Real-Or-Random (ROR) model [29]. According to this model, the malicious intruder $\mathcal{A}$ requires to distinguish the original session key against any random integer in an authenticated key exchange (AKE) protocol. The ROR model has become popular among the research community for application in respective AKE protocols. Based on this property, the ROR model is helpful to prove the security of the session key (SK) for AKE protocol.

1) ROR Model: Our contributed model's security relies on the following hardness of the one-way cryptographic collision resistant hash function.

Definition 1: One way collision resistant hash function A cryptographic collision-defiant one-way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^l$, being a deterministic algorithm, produces an outcome of a binary string of length l after taking an input of string of random length [34]. If $Adv^h_{\mathcal{A}}(t)$ is the advantage of the malicious intruder for evaluating hash-collisions in time t then,

$$Adv^{hash}_{\mathcal{A}}(t) = Pr[(\beta_1, \beta_2) \Leftarrow_R A : \beta_1 \neq \beta_2, h(\beta_1) = h(\beta_2)]$$

where $(\beta_1, \beta_2) \Leftarrow_R$ shows that the parameters β_1 and β_2 are selected on random basis by the adversary. An $(\overline{\omega}, t)$ - adversary $\mathcal{A}$ intending to influence the collision resistance feature of $h(.)$ function signifies that $Adv^{hash}_{A}(t) \leq \overline{\omega}$ holds true given at most time t [34], [35].

2) Security Model: Before demonstrating the proof regarding the session key's security, we describe the ROR model [36]. Participants: We assume the entities V_i^x, HAP_j^y and CS_k^z be the x^{th} instance of vessel V_i, y^{th} instance of HAP_j and z^{th} instance of CS_k, respectively. These instances are termed as oracles.

a) Accepted state: If an instance V_i^x, approaches the accepted state upon receiving the last message in the protocol, it is said to be in the accepted state. For every session, a session identifier sid for V_i^x, is produced by concatenating all exchanged messages in order. Partnering: We assume, the instances V_i^x, and HAP_j^y are partners of each other, and those instances must support the following conditions: 1) both of the instances V_i^x and HAP_j^y are in accepted state; 2) the instances V_i^x and HAP_j^y validate the authenticity of each other under the same sid; 3) both V_i^x, and HAP_j^y, stand mutual partners to each other.

b) Freshness: The instances V_i^x, and HAP_j^y, are deemed fresh if the established session key between vessel V_i and HAP_j is not revealed to the adversary. In CK-based adversary model [32], adversary $\mathcal{A}$ controls all communicative messages exchanged among the parties and is also familiar with most of the initialized factors in the maritime system. Furthermore, the adversary might modify and intercept all communication messages exchanged on the public channel and manipulate the new messages in the system. The adversary may employ the following oracle queries:

c) $Execute(V_i^x, HAP_j^y, CS_k^z)$: The execute query, as an eavesdropping attack, allows the adversary to intercept all communication messages $\{M_{vhc}, M_{hc}, M_{chv}, M_{hv}\}$ exchanged on the public channel.

d) $Reveal(V_i^x, HAP_j^y)$: After the execution of reveal query, the session key SK constructed between V_i^x and its partner HAP_j^y is exposed to adversary $\mathcal{A}$.

e) $Send(V_i^x, M)$: The send query models active attack by the adversary. Upon executing this query, the message M could be submitted by the adversary to its participating instance V_i^x.

f) $Corrupt(V_i^x)$: Using this query, an adversary can acquire all of the verifiers and secret credentials as stored in the stolen smart card of the legal participating instance V_i^x.

g) $Test(V_i^x, HAP_j^y)$: Using this query, the semantic security of the established session key SK between V_i^x and HAP_j^y is modeled. An unbiased coin $c \in \{0,1\}$ is flipped at the beginning of the experiment and is kept secret, whose resultant value may play a crucial role in obtaining the output of the query if the outcome is close to query result of an adversary. If the session key is not established or the V_i^x instance is not fresh, it would return a null value ($\perp$). On the other hand, if $c = 1$, either the instance V_i^x or HAP_j^y would return the session key SK to the adversary $\mathcal{A}$. If $c = 0$, it would return a random integer to the adversary.

It is worth noting that all of the participants, inclusive of the adversary, might access the cryptographic one-way collision-resistant hash algorithm $h(.)$. Here, the hash algorithm $h(.)$ behaves like a random oracle. We used a difference lemma [37] to analyze the security of the authentication model formally.

Lemma 1 (Difference Lemma): We assume that R, S and F represent the events as described in a probability distribution, and we assume that $R \wedge \neg F \leftrightarrow \wedge \neg F$. Then $Pr[R] - Pr[S] \leq Pr[F]|$.

Theorem 1: We assume that a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ runs in time t against the proposed protocol AKA scheme. D is represented as a password dictionary having uniform distribution, while $|D|$ denotes the size of D. The q_{hs} and q_{sd} denote the number of $hash$ and $send$ queries. The $|hash|$ represents the $h(.)$ function range, while l shows the resultant hash value's length. The $Adv_{\mathcal{A}}^{hash}$ depicts the advantage of adversary $\mathcal{A}$ for breaking the hash problem having upper bound time t. Hence the advantage of an adversary to break the security of session key for contributed AKA model can be shown as:

$$Adv_{\mathcal{A}}^{AKA} \leq \frac{q_{hs}^2}{|hash|} + \frac{q_{sd}^2}{2^l - 1.|D|} + Adv_{\mathcal{A}}^{hash}(t) \tag{1}$$

Proof: We used five games $Gm_i, i = 0, 1, 2, 3, 4$ to verify that the contributed model is provable secure. We assume SC_{Gm_i} to be the success rate in guessing about c for game Gm_i, while the corresponding advantage of adversary $\mathcal{A}$ in guessing that value is defined as $Pr[SC_{Gm_i}]$.

Game Gm_0: In Gm_0, the adversary performs a real attack experiment against the contributed model in random oracle model (ROM). The adversary selects the random value for c integer at the beginning of the trial. Per the illustration of semantic security [38],

$$Adv_{\mathcal{A}}^{AKA} = |2.Pr[SC_{Gm_0}] - 1| \tag{2}$$

Game Gm_1: The Gm_1 behaves as an eavesdropping attempt in which the adversary models the attack by executing $Execute(V_i^x, HAP_j^y, CS_k^z)$ oracle query. The adversary can intercept all of the messages, i.e. $M_{vhc} = PID_i, P_{vi}, Q_{vi}, t_i$, $M_{hc} = \{HID_j, M_{vhc}, P_{hj}, t_{hj}\}$, $M_{chv} = \{R_{CH}, R_{CV}, V_{CH}, V_{CV}, t_{ck}\}$ and $M_{hv} = \{R_{CV}, V_{CV}, t_{hj}^2\}$ during the exchange of communication messages among V_i, HAP_j, and CS_k. Thereafter, the adversary executes $Test(V_i^x, HAP_j^y)$ oracle-based query. Upon evaluating the query output, the adversary may infer whether he is exporting the legal session key SK or any random integer. Then the session key SK is calculated between V_i and HAP_j as $SK_{cv} = h(r_{vi}||r_{ck}||X_i||VID_i)$, where $r_{vi} = Y_i \oplus Q_{vi}$ and r_{ck} is a random integer. If the adversary attempts to compute the session key SK after manipulating these message parameters, it must access the r_{ck} parameter through R_{CV} factor, i.e., $R_{CV} = E_{X_i}(r_{ck}, PID_i^{nw}, t_{ck})$. However, to recover it must have access to X_i, a long-term secret, which V_i or CS_k only possesses. Therefore, after interception or eavesdropping of the messages, the adversary may not be able to increase its chances of winning the game Gm_1. Thus, we have

$$Pr[SC_{Gm_0}] = Pr[SC_{Gm_1}] \tag{3}$$

Game Gm_2: The Gm_2 is similar to the Gm_1. However, it is compounded with $Send(V_i^x, M)$ and $h(.)$ oracles simulation. The Gm_2 is modeled as an active adversary where the adversary attempts to deceive a participating member into accepting the message that it had crafted or modified. Despite this, the adversary may constantly execute hash oracle queries to verify any possibility of collision in the messages. However, each of those messages $\{M_{vhc}, M_{hc}, M_{chv}, M_{hv}\}$ is embedded with fresh timestamps, randomly defined integers, and the identities of participating members. Thus, there exists no collision on issuing $Send$ oracle queries by the adversary. Referring to the birthday paradox, we get to the following relationship:

$$Pr[SC_{Gm_0}] - Pr[SC_{Gm_1}] \leq \frac{q_{hs}^2}{2|hash|} \tag{4}$$

Game Gm_3: The inclusion of $Corrupt(V_i^x)$ oracle query distinguishes between Gm_3 and Gm_2 games. In this context, the adversary might gain all of the secret parameters such as $\{VID_i, PID_{vi}, X_i, Y_i\}$ from the memory of vessel V_i. If the adversary attempts to guess the short-term secret r_0 from these parameters, it must access long-term secrets such as K_C. In case, A executes q_{sd} times the $Corrupt$ oracle queries to guess the K_C, and reaches the upper bound, then the probability of the adversary winning the game Gm_3 is:

$$Pr[SC_{Gm_3}] - Pr[SC_{Gm_2}] \leq \frac{q_{sd}^2}{2^l|D|} \tag{5}$$

Game Gm_4: In the final game, Gm_4, the adversary attempts to compute session key $SK_{cv} = h(r_{vi}||r_{ck}||X_i||VID_i)$ by employing the short term secrets such as r_0, VID_i or timestamps. It will be a hard problem to guess due to collision resistant property of hash function in time t. However, for deriving r_{ck} it must have access to X_i secret and long-term KC secret that the legal participants only possess. Hence, we get to the relationship as given below:

$$Pr[SC_{Gm_4}] - Pr[SC_{Gm_3}] \leq Adv_{\mathcal{A}}^{hash}(t) \tag{6}$$

Finally, the adversary models all oracles, and the former is only left for guessing the value of c integer to win the game after issuing the query $Test(V_i^x, HAP_j^y)$. Hence, the $Pr[SC_{Gm_4}]$ beholds the probability for guessing the integer c, as shown below:

$$= Pr[SC_{Gm_4}] - \frac{1}{2} \tag{7}$$

Using equations (2) and (3), we get

$$\begin{aligned} Adv_{\mathcal{A}}^{AKA} &= 2.|Pr[SC_{Gm_0}] - \frac{1}{2}| \\ &= 2.|Pr[SC_{Gm_1}] - |Pr[SC_{Gm_4}] \end{aligned} \tag{8}$$

Referring to the above equations (4)-(6) in consideration with triangular inequality, we have the relation as follows:

$$\begin{aligned} &= |Pr[SC_{Gm_4}] - |Pr[SC_{Gm_1}]| \\ &\leq |Pr[SC_{Gm_4}] - |Pr[SC_{Gm_3}]| + |Pr[SC_{Gm_3}] \\ &\quad -|Pr[SC_{Gm_1}]| \\ &\leq |Pr[SC_{Gm_4}] - |Pr[SC_{Gm_3}]| + |Pr[SC_{Gm_3}] \\ &\quad -|Pr[SC_{Gm_2}]| \\ &\quad +|Pr[SC_{Gm_2}] - |Pr[SC_{Gm_1}]| \\ &\leq \frac{q_{hs}^2}{2|hash|} + \frac{q_{sd}^2}{2^l.|D|} + Adv_{\mathcal{A}}^{hash}(t) \end{aligned} \tag{9}$$

Using equations (8) and (9), we get the following result as shown in equation (10)

$$Adv_{\mathcal{A}}^{hash}(t) \leq \frac{q_{hs}^2}{2|hash|} + \frac{q_{sd}}{2^{l-1}.|D|} + 2Adv_{\mathcal{A}}^{hash}(t) \quad (10)$$

B. Informal Analysis

This section provides discussions on the security provision of the proposed LSMP-MTS.

1) Mutual Authentication: In contributed model, both entities such as V_i and CS_k mutually verify each other with the help of HAP_j. After the receipt of M_{vhc} and M_{hc}, the CS_k checks the freshness of timestamp t_{hj} and verifies t_{hj} after computing K_{HC} and decrypting P_{hj} using K_{HC}. Upon verification, it further decrypts PID_i and computes X_i, Y_i to recover r_{vi} from Q_{vi}. Now it checks the validity of the computed $P_{vi} = h(X_i||VID_i||t_{vi}||r_{vi})$ through matching with the received P_{vi} from V_i. In this way, CS_k verifies V_i based on K_C and computed K_{HC}. The CS_k knows that a legal PID_i can only be presented by a legitimate vessel; hence it authenticates the vessel on the basis of PID_i. Likewise, the V_i authenticates CS_k based on verification of V_{CV}. It understands that the session key $SK_{cv} = h(r_{vi}||r_{ck}||X_i||VID_i)$ can only be constructed by a valid CS_k having access to X_i and VID_i, while the construction of V_{CV} also depends upon the same SK_{cv}. Thus, both entities successfully authenticate one another in the contributed scheme.

2) Vessel Anonymity: The contributed model ensures anonymity for the vessel. This is because the identity of the vessel V_i remains hidden in PID_i in the form of $PID_i = E_{KC}(VID_i, r_0)$, which acts as a pseudo-identity for V_i and is submitted to the HAP_j during authentication request. Only CS_k may derive the identity of V_i by decrypting PID_i using its private secret key K_C, which may later be used in computing a crucial factor parameter X_i to proceed in the scheme. Hence our scheme supports anonymity.

3) Untraceability: The adversary does not trace the proposed scheme at all since all of the parameters utilized in the protocol's communication messages remain distinctive across various sessions. The adversary must derive a common link across the messages of various sessions among the same participants to trace a particular subscriber. The reason being the contributed protocol utilizes pseudo-identity PID_i that is updated in each session among the participants. Hence, our scheme remains fully untraceable among various sessions of the same participants.

4) Stolen Verifier Attack: If the repository of verifiers is stolen on the server's end, it may lead to serious threats to reveal previous session keys of the subscribers. However, in the proposed scheme, the Control Server CS_k does not maintain any repository for vessels V_i, except the counter CN on each HAP_j. An adversary cannot exploit the CN for any malicious purpose until it gains access to a private secret key of CS_k, i.e., K_C, which is assumed to be protected and cannot be easily guessed.

5) Ephemeral Secret Leakage Threat: In contributed scheme, both V_i and CS_k build an agreed session key $SK_{cv} = h(r_{vi}||r_{ck}||X_i||VID_i)$. In case the ephemeral secrets such as r_{vi} or r_{ck} are exposed to the adversary, still, the latter may not compute the session key. The reason being, the session key $SK_{cv} = h(r_{vi}||r_{ck}||X_i||VID_i)$ requires a long-term secret X_i as well as the vessel's identity VID_i. In the absence of these secrets an adversary cannot create a valid session key SK_{cv}. Therefore, our scheme is resistant to ephemeral secret leakage threat.

6) Forward and Backward Secrecy: In contributed model, even if the particular session key SK_{cv} is exposed to the adversary, the latter may not calculate previous or future session keys using this current session key. This is because it cannot recover short term secret, i.e., r_{vi}, or long term secret, i.e., X_i using the exposed session key SK_{cv} along with intercepted messages. Hence our scheme supports forward as well as backward secrecy.

7) Impersonation Attack: If an adversary attempts to impersonate either V_i or CS_k, it will be traced on both ends. Suppose, in proposed scheme if $\mathcal{A}$ attempts an impersonation attack by crafting a fake message $M_{vhc} = \{PID_i, P_{vi}, Q_{vi}, t_{vi}\}$. Then, CS_k may foil this attempt by verifying P_{vi}. Obviously, an adversary might not access valid X_i, VID_i parameters and will be unable to design a legal M_{vhc} with a fresh timestamp t_{vi}. Likewise, if $\mathcal{A}$ attempts to forge a message $M_{hv} = \{R_{CV}, V_{CV}, t_{hj}^2\}$ to impersonate as CS_k, the V_i may thwart this attack by computing $SK_{cv} = h(r_{vi}||r_{ck}||X_i||VID_i)$ and verifying $V_{CV} = \{SK_{cv}||r_{vi}||r_{ck}||PID_i^{new}\}$. Since, V_i knows that an adversary can neither produce a legal r_{vi} factor nor compute a valid SK_{cv} for lacking access to X_i parameter. Therefore, the contributed model is immune to forgery attacks.

8) Replay Attack: Suppose an adversary intercepts the messages on insecure open channel and attempts to replay those messages to other legitimate entities for impersonation. In that case, it may not be successful on the grounds of employed timestamps. Every communication message is embedded with fresh timestamps such as t_{vi}, t_{hj}, t_{ck}, t_{hj}^2. Due to these timestamps, if an adversary attempts to replay a message, it will be diagnosed at the end of receiving participant by checking its freshness and verification in the hash-based or encrypted message. For instance, the CS_k clears the reservation of any replay threat by verifying the freshness of t_{hj} and verifying the same through decrypting P_{hj} with key K_{HC}. After checking the decrypted timestamp t_{hj}, the CS_k eliminates the possibility of a replay attack. Similarly, the V_i checks as well as verifies the timestamp t_{hj}^2 to authenticate HAP_j and ultimately CS_k. Hence our scheme is resistant to replay attacks.

9) Man-in-the-Middle Attack: It is evident from the subsection illustrating resistance of the scheme against impersonation threats. Thus if an adversary attempts to modify the parameters or craft new factors, it will not be able to initiate a man-in-the-middle (MIDM) attack as both participants, V_i and CS_k mutually authenticate one another. If the adversary attempts to construct $M_{vhc} = \{PID_i, P_{vi}, Q_{vi}, t_{vi}\}$ to generate a mutually agreed session key with the legal CS_k, it will not be successful in this attempt due to lacking X_i as well as VID_i parameters. Similarly, If $\mathcal{A}$ attempts to construct $M_{hv} = \{R_{CV}, V_{CV}, t_{hj}^2\}$ for generating an agreed session key,

TABLE II
SECURITY FEATURES

	[25]	[23]	[26]	[22]	[24]	[18]	Our
SF_1	✗	✓	✗	✓	✗	✓	✓
SF_2	✓	✗	✗	✗	✓	✓	✓
SF_3	✗	✓	✓	✓	✓	✓	✓
SF_4	✗	✗	✓	✗	✓	✓	✓
SF_5	✓	✗	✓	✓	✓	✓	✓
SF_6	✓	✓	✓	✓	✓	-	✓
SF_7	✓	✓	✓	✓	✓	✓	✓
SF_8	✗	✓	✓	✓	✓	✓	✓
SF_9	✓	✓	✓	✓	✓	✓	✓
SF_{10}	✗	✓	✓	✓	✓	✓	✓
SF_{11}	✗	✓	✓	✓	✓	-	✓
SF_{12}	✓	✓	✓	✓	✓	✓	✓
SF_{13}	✓	✓	✓	✓	✓	✓	✓
SF_{14}	✓	✓	✗	✗	✓	-	✓

Note: SF_1: Supports Anonymity and untraceability, SF_2: Supports mutual authentication, SF_3: Offline-Password guessing attack, SF_4: User/Server impersonation attack, SF_5: Replay attack, SF_6: Man-in-the-middle attack, SF_7: Ephemeral information leakage attack, SF_8: Supports forward/backward secrecy, SF_9: Stolen verifiers attack, SF_{10}: Device capture attack, SF_{11}: Drone capture attack, SF_{12}: Resist Denial of service attack, SF_{13}: Resist Desynchronization attack, SF_{14}: Supports session key security; ✓: Resists attack-/Supports security property, ✗: Do not resist attack or support security feature.

it may not do so without accessing X_i parameter. Hence, our scheme is immune to MIDM attacks.

V. PERFORMANCE EVALUATION

This section analyzes the security traits and evaluates the performance by comparing [18], [22]–[26] against the proposed protocol concerning computational cost, communication cost, and security functions. The comparison of security functions for [18], [22]–[25] and proposed scheme is exhibited in Table II. The schemes [24]–[26] do not support anonymity and untraceability features. Mutual authentication is not assured by [22], [23], [26]. The scheme [25] is prone to offline-password guessing attacks, device capture attacks, and not supporting forward secrecy. Similarly, [22]–[24] are vulnerable to forgery attacks, while [23] does not resist replay attacks. Our scheme is secure from all these attacks as well as maintains efficiency. The computational costs of [18], [22]–[26] and the proposed scheme are shown in Table III. To evaluate the computational cost for IoT devices on the vessel, HAP_j, and server CS_k, we base our operations cost on the experiment conducted by Hussain *et al.* in [28], and assume the same computational costs. The computational primitives such as hash function, symmetric encryption or decryption, bilinear operation, and fuzzy extractor are represented by T_h, T_{ed}, T_b, T_{fe}, respectively. The cost of T_h, T_{ed}, T_b operations in milliseconds for device, server and drone/HAPS are $\{0.009, 0.017, 17.36\}$, $\{0.004, 0.08, 4.038\}$, and $\{0.006, 0.013, 12.52\}$ respectively. Here, the T_{fe} is equivalent to $5.116ms$.The schemes [18], [22]–[26] bear the total computational cost of $17T_h + 6T_b$, $31T_h + 1T_{fe}$, $24T_h$, $58T_h + 1T_{fe}$, $19T_h$, $32T_h$, with $84.37ms$, $5.334ms$, $0.16ms$, $18.699ms$, $0.121ms$, and $0.211ms$, respectively. The proposed scheme bears total computational cost of $13T_h + 7T_{ed}$ operations with $0.243ms$. It is obvious, [23], [25], [26] incur less computational cost than our scheme. However, these are vulnerable to many threats, as shown in Table II. Although [18] is resistant to attacks, it is inefficient for the high computational cost of bilinear operations. The schemes [22], [24] are not only costly but also prone to security threats. Table IV depicts the comparison for communication costs of proposed and comparative schemes [18], [22]–[26]. We assume the identities and hash, secure hash standard (SHA-1) takes 160 bits respectively. The randomly generated integers take 128 bits, while the timestamps take 32 bits. It is apparent from Table IV that the proposed protocol bears 2624 bits of communication cost, which is less than [25], [26] bearing 2720 bits and 2752 bits, respectively. Although the schemes [22]–[24] bear less computational cost of 1696 bits, 1472 bits, 1536 bits, respectively, than the proposed scheme, however, these schemes go through many security-based limitations as depicted in Table II. In the light of analysis portrayed in the form of security features, computational and communicational analysis, the proposed scheme may find its practical suitability in the maritime ecosystem.

TABLE III
COMPUTATIONAL COSTS

Scheme	User/ Device	Server/ GSS	Drone/ HAP_j/ AP	Latency (ms)
[25]	$7T_h$	$7T_h$	$5T_h$	≈ 0.121
[23]	$10T_h$	$7T_h$	$7T_h$	≈ 0.16
[26]	$11T_h$	$7T_h$	$14T_h$	≈ 0.211
[22]	$16T_h + 1T_{fe}$	$8T_h$	$7T_h$	≈ 5.334
[24]	$14T_h$	$14T_h$	$30T_h + 1T_{fe}$	≈ 18.699
[18]	$5T_h + 2T_b$	$3T_h + 2T_b$	$9T_h + 2T_b$	≈ 84.37
Our	$3T_h + 1T_{ed}$	$3T_h + 1T_{ed}$	$7T_h + 5T_{ed}$	≈ 0.243

TABLE IV
COMMUNICATION COST ANALYSIS

Scheme.→	[25]	[23]	[26]	[22]	[24]	[18]	Our
Bits Exch.	2720	1472	2752	1696	1536	1920	2624

VI. CONCLUSION

6G-IoT enabled MTS 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 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., Real-Or-Random (ROR) oracle model. Also, a detailed comparison study is conducted to assess the feasibility of the proposed scheme. The results from both studies reveal that the proposed scheme outperforms its counterpart schemes in terms of security toughness and has a better security-to-efficiency tradeoff.

REFERENCES

[1] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[2] Y. Huo, F. Lu, F. Wu, and X. Dong, "Multi-beam multi-stream communications for 5G and beyond mobile user equipment and UAV proof of concept designs," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–5.

[3] K. Lou, Y. Yang, E. Wang, Z. Liu, T. Baker, and A. K. Bashir, "Reinforcement learning based advertising strategy using crowdsensing vehicular data," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4635–4647, Jul. 2021.

[4] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: A survey," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102177.

[5] H. Huang, S. Guo, W. Liang, K. Wang, and A. Y. Zomaya, "Green data-collection from geo-distributed IoT networks through low earth-orbit satellites," *IEEE Trans. Green Commun. Netw.*, vol. 3, no. 3, pp. 806–816, Sep. 2019.

[6] Y. Huo, X. Dong, and S. Beatty, "Cellular communications in ocean waves for maritime Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9965–9979, Oct. 2020.

[7] A. Munusamy *et al.*, "Edge-centric secure service provisioning in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 12, 2021, doi: 10.1109/TITS.2021.3102957.

[8] G. Raja, A. Ganapathisubramaniyan, S. Anbalagan, S. B. M. Baskaran, K. Raja, and A. K. Bashir, "Intelligent reward-based data offloading in next-generation vehicular networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3747–3758, May 2020.

[9] J. O. Eichenhofer, E. Heymann, B. P. Miller, and A. Kang, "An in-depth security assessment of maritime container terminal software systems," *IEEE Access*, vol. 8, pp. 128050–128067, 2020.

[10] Y. Guo, M. Wu, K. Tang, J. Tie, and X. Li, "Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6557–6564, Jul. 2019.

[11] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.

[12] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Proc. IEEE Int. Symp. Saf., Secur. Rescue Robot. (SSRR)*, Shanghai, China, Oct. 2017, pp. 194–199.

[13] S. P. Arteaga, L. A. M. Hernandez, G. S. Perez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS spoofing vulnerability in the drone 3DR Solo," *IEEE Access*, vol. 7, pp. 51782–51789, 2019.

[14] Z. Feng *et al.*, "Efficient drone hijacking detection using onboard motion sensors," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2017, pp. 1414–1419.

[15] M. A. Khan *et al.*, "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Trans. Ind. Informat.*, early access, Aug. 4, 2021, doi: 10.1109/TII.2021.3101651.

[16] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354.

[17] M. Rodrigues, J. Amaro, F. S. Osorio, and B. R. L. J. C. Kalinka, "Authentication methods for UAV communication," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Barcelona, Spain, Jun. 2019, pp. 1210–1215.

[18] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, Apr. 2020.

[19] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101955.

[20] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2982–2994, Oct. 2021.

[21] R. Arul, G. Raja, A. K. Bashir, J. A. Chaudry, and A. Ali, "A console GRID leveraged authentication and key agreement mechanism for LTE/SAE," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2677–2689, Jun. 2018.

[22] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.

[23] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020.

[24] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Oct. 2019.

[25] M. Turkanovi'c, B. Brumen, and M. Hölbl, "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.*, vol. 20, pp. 96–112, Sep. 2014.

[26] M. S. Farash, M. Turkanovi'c, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[27] F. Al-Turjman, Y. K. Ever, E. Ever, H. X. Nguyen, and D. B. David, "Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks," *IEEE Access*, vol. 5, pp. 24617–24631, 2017.

[28] S. Hussain, K. Mahmood, M. K. Khan, C.-M. Chen, B. A. Alzahrani, and S. A. Chaudhry, "Designing secure and lightweight user access to drone for smart city surveillance," *Comput. Standards Interface*, vol. 80, Mar. 2022, Art. no. 103566.

[29] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–19, Jun. 2021.

[30] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107731.

[31] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102502.

[32] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2001, pp. 453–474.

[33] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[34] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, pp. 1–16, Dec. 2010.

[35] D. R. Stinson, "Some observations on the theory of cryptographic hash functions," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 259–277, Feb. 2006.

[36] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.* Springer, 2005, pp. 65–84.

[37] V. Shoup, "Sequences of games: A tool for taming complexity in security proofs," *IACR Cryptol. ePrint Arch.*, vol. 2004, p. 332, Nov. 2004.

[38] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1654–1667, 2019, doi: 10.1109/TIFS.2019.2946933.

Shehzad Ashraf Chaudhry received the master's and Ph.D. degrees (Hons.) from the International Islamic University, Islamabad, Pakistan, in 2009 and 2016, respectively. He has authored over 140 scientific publications appeared in different international journals and proceedings, including more than 105 in SCI/E journals. With an H-index of 33 and an i10-index of 67, his work has been cited over 3000 times. He was a recipient of the Gold Medal for achieving a 4.0/4.0 CGPA in his master's. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among top productive computer scientists in Pakistan. For the consecutive two years (i.e., 2020 and 2021), he is being listed among the top 2% computer scientists across the world in Stanford University's report.

Azeem Irshad received the Ph.D. degree from the International Islamic University, Islamabad, Pakistan. He has authored more than 75 international journals and conference publications, including 40 SCI-E journal publications. His research work has been cited over 970 times with 15 H-index and 22 i10-index. He received the Top Peer-Reviewer Award from Publons in 2018 by serving more than 60 reputed international journals.

Muhammad Asghar Khan received the Ph.D. degree in electronic engineering from the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He works as an Assistant Professor with the Department of Electrical Engineering, Hamdard University, Islamabad. He is a reviewer for various journals published by IEEE, Elsevier, MDPI, and EURASIP. He has served as a guest editor for a number of international journals.

Sajjad Ahmad Khan has received the B.S. degree in information technology from the University of Engineering and Technology (UET), Peshawar, in 2007, the M.S. degree in telecommunication and networking from IQRA University, Islamabad, Pakistan, in 2011, and the Ph.D. degree in computer engineering from Kocaeli University, Turkey, in 2020. Currently, he is working as a Post-Doctoral Researcher at Istanbul Technical University (ITU), Turkey, under a TUBITAK Project. He is also associated with the Department of Software Engineering, Istanbul Gelisim University, İstanbul, Turkey. He has published over a dozen of articles in prestigious journals and conferences. He was supported by the "2232 International Fellowship for Outstanding Researchers Program of TUBITAK" (Project No: 118C276), Turkey. His research interests are radio resource management (RRM), interference management, mobility management, dual connectivity, mmWave, the IoT, cooperative communication, and machine learning in LTE-A, 5G, and beyond heterogeneous network (HetNet) systems. He is an active reviewer of many conferences and journals.

Summera Nosheen (Member, IEEE) received the Ph.D. degree from the School of Electrical Engineering and Computing, The University of Newcastle, Australia, in 2021. Her research interests include wireless networks, quality of service, quality of experience, and MAC layer resource allocation. She received the University of Newcastle International Postgraduate Research Scholarship and the University of Newcastle Research Scholarship in 2017. She was the recipient of the first position in master's degree.

Ahmad Ali AlZubi received the Ph.D. degree from the National Technical University of Ukraine (NTUU). He is a Full Professor at King Saud University (KSU). His current research interests include computer networks, cloud computing, big data, and data extracting. He is a certified member of the Board of Assessors of Quality Management System at King Saud University (BOA-QMS).

Yousaf Bin Zikria (Senior Member, IEEE) is currently working as an Assistant Professor with the Department of Information and Communication Engineering, College of Engineering, Yeungnam University, Gyeongsan-si, South Korea. He has authored more than 100 peer-reviewed articles, conferences, book chapters, and patents. His cumulative journal impact factor is more than 300. He has been listed in the world's top 2% researchers/scientists published by Elsevier and Stanford University.