



Nuclear resilient and redundant compute and communication integrated network

A. A. Periola¹

Accepted: 11 December 2023 / Published online: 23 January 2024
© The Author(s) 2024

Abstract

Future communication networks use computing platforms i.e., data centers for enabling content access. The operation of data centers is evolving to meet new requirements such as reducing the operating cost. The use of data centers is recognized to have significant challenges due to high operating costs. The high operating costs arises due to the necessity of data center cooling. The cooling costs can be reduced by siting data centers in the underwater environment. In the underwater environment, data centers are cooled by freely available cold water. However, siting data centers in the underwater environment exposes them to risk from other underwater applications. The use of underwater data centers is susceptible to service loss due to the launch of missiles from submarines in defense applications. Underwater data centers are susceptible to service loss from the launch of missiles from submarines. Hence, it is necessary to design a network architecture that ensures continued service delivery when nuclear attacks occur. The presented research proposes a novel network architecture enabling service continuity in the underwater data center. The proposed architecture incorporates resiliency and comprises terrestrial and non-terrestrial data centers. The proposed network architecture incorporates redundancy and utilizes terrestrial and non-terrestrial data centers. In addition, the research presents a protocol enabling co-existence between underwater data centers and missile launching submarines used in defence applications. The research formulates and evaluates the operational duration, number of packets forwarding paths, and computing resource utilization as the metrics. Performance evaluation shows that the proposed network architecture improves the operational duration and computing resource utilization by an average of (27.7–71.5)% and (23.5–44.2)%, respectively. Furthermore, the proposed network architecture enables the realization of more resilient paths. The use of more resilient paths enhances packet transmission. Evaluation shows that the proposed network architecture enhances the number of resilient packets forwarding paths by (18.2–57.4)% on average.

Keywords Internet · Resilient architecture · Nuclear attacks · Missiles · Data centers

1 Introduction

Cloud computing platforms plays a key role in enabling low-latency content access on the internet (Saba et al. 2023; Das and Inuwa 2023; Wen et al. 2023) because of their crucial role in enabling content access to subscribers (Ensan et al. 2021; Kliks et al. 2017; Lingshu et al. 2021). The realization of low latency has necessitated the design

and use of terrestrial data centers. In this regard, the use of underwater data centers reduce latency for coastal network subscribers (<https://news.microsoft.com/features/microsoft-research-project-puts-cloud-in-ocean-for-the-first-time/>). The use of underwater data centers faces threats from submarine ballistic missile (Johnson 2023; Ellison et al. 2023; Kirchberger 2023; Kristensen et al. 2023). The threat should be addressed because of the increasing use of missiles and associated weapons (Kristensen et al. 2023; Kristensen and Korda 2023).

Therefore, the underwater data center faces challenges as regards continued service delivery due to the use of submarine launched missiles. However, the existing research has not presented network architecture ensuring

✉ A. A. Periola
periola@cpur.ac.za

¹ Electrical, Electronic, and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa

the continuity and survivability of underwater data center functionality. The design of a network that enables continued service delivery from underwater data centers when missiles are launched from the ocean is proposed. In this case, the underwater data center is a network entity whose functionality is highly susceptible to nuclear attacks from submarine launched missiles.

Research Contribution The use of underwater data center as the cloud component in future networks is recognized to be beneficial due to the reduced operational costs. Existing work recognizes that the use of underwater data center reduces the cooling cost. The cooling cost is reduced due to the benefits of accessing freely available ocean water. The use of underwater data center also reduces content access latency for coastal subscribers to communication networks. However, the location of underwater data center in the underwater environment increases their exposure to challenges from other applications in the underwater environment. An important application in this regard is underwater submarines that launch missiles. It is important to ensure that the performance of underwater data center does not experience challenges from submarine launched missiles. The presented research addresses two concerns. The first concern is the design of a network architecture enabling continued service provisioning of underwater data centers. The second concern is formulating and evaluating the performance benefit of the proposed network architecture. The discussion here makes the following contributions:

1. First, the paper proposes a network architecture enabling subscribers to have access to cloud functionality in the event of nuclear missile attacks. The attacks arise from submarine-launched missiles that disrupt underwater data center functionality. The paper proposes an architecture that implements redundancy for underwater data centers in a communications network. The proposed network architecture enables the survivability of future networks. The concerned future networks comprise underwater computing platforms. The underwater computing platforms can experience potential loss in function due to the occurrence of missile attacks. The network realizes survivability via redundancy pairs where an underwater data center is associated with other data centers. In the proposed network, the redundant data center can be another underwater data center, a terrestrial data center or a stratosphere data center. Locations in the underwater and stratosphere are beneficial because they benefit from free cooling (stratospheric cooling in stratosphere data centers). The novelty of the proposed research lies in the design of a network architecture for underwater data center in the event of a nuclear attack. Currently,
2. Second, the paper presents a nuclear-underwater data center co-existence protocol. In this protocol, the submarine with missile weapon payload is deployed considering the existence of underwater data centers. The proposed co-existence protocol advocates that underwater data centers should be placed out of locations where they intersect with least hydrodynamic drag path. This is done to ensure that the underwater data centers are not in the potential path of submarine launched missiles.
3. Third, the paper formulates the performance benefits of the proposed architecture enabling survivability for underwater data centers. The underwater data centers have redundant data centers in the proposed communication network. The formulated metrics are (1) Data center uptime (functional duration), (2) Computing resource utilization, and (3) Number of Packets Forwarding Paths. The existing case is one in which only underwater data centers are realized in a network without redundancy. Currently, existing work in <https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter> recognizes that underwater data centers have a low failure probability. However, this has not considered the threat arising from submarine ballistic missiles. The proposed case is one in which underwater data centers are used while incorporating redundancy. Furthermore, the paper examines the performance benefit of the proposed network architecture incorporating redundancy. This is done via simulation of scenarios associated with the existing case and proposed case.

The rest of the proposed research as presented in the paper is organized in the following manner: Sect. 2 describes the existing and background work. Section 3 presents the problems being addressed. Section 4 discusses the proposed solution. Section 5 formulates the performance model. Section 6 discusses the results of performance simulation. Section 7 is the conclusion.

2 Existing and background work

The discussion in this section focuses on the existing role of underwater data centers and examines the influence of the surrounding ocean environment. It has two aspects. The first aspect presents the role of underwater data centers and considers the influence of the underwater environment on their performance. The second aspect examines underwater

data centers from the perspective of survivable communication networks.

2.1 Underwater data centers: roles and influence of the underwater environment

The description of the performance of underwater data centers is provided in <https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter>. The discussion in <https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter> notes that the underwater data center has a lower failure rate in comparison to a terrestrial data center. In this case, the underwater data center is observed to have a lower failure rate than the terrestrial data center. The failure rate is 87.5% lower than the failure rate of the existing terrestrial data center. The reduced failure rate arises due to the use of dry nitrogen. Additional observation in <https://earth.org/underwater-data-centres/>, Cutler et al. (2017) and Hu et al. (2022) show that underwater data centers comprising multiple servers have a reduced failure rate. The discussion in Cutler et al. March (2017) and Hu et al. (2022) recognize that underwater data center design has a robust performance against certain failure causing events. Cutler et al. (2017) notes that using renewable underwater energy provides a robust solution against electric grid failure.

In addition, Cutler et al. (2017) note that hardware failures should be addressed and fixed autonomously. This task is being executed using autonomous methods applicable to conventional data centers. It is implicitly assumed that failures arise due to two events. These events are server component and electrical grid malfunction. A mechanism of identifying the threat and designing a malfunction prevention mechanism is required in a manner. The mechanism should consider threats arising from the peculiarities of the underwater environment.

Hu et al. (2022) discuss the robustness of underwater data centers against subsystem failure. This is done with focus on the role of the power and cooling system. The discussion in Hu et al. (2022) describes an approach enabling the underwater data center to maintain the robustness of the power and cooling system. The focus in Hu et al. (2022) is like that in Cutler et al. (2017) and considers component level outputs that can cause underwater data center performance failure. It has not considered external systems in the ocean environment that can induce underwater data center performance failure. Additional consideration in <https://spectrum.ieee.org/want-an-energyefficient-data-center-build-it-underwater> and (<https://www.euronews.com/next/2022/08/31/underwater-data-centres-are-coming-can-they-slash-co2-emissions-and-make-the-internet-fast>) shows that underwater data centers have received significant consideration due to the low-cost

cooling benefit. In addition, there is an implicit assumption that underwater data centers have a low failure rate. This notion is found in Cutler et al. (2017), Hu et al. (2022), <https://spectrum.ieee.org/want-an-energyefficient-data-center-build-it-underwater>; <https://www.euronews.com/next/2022/08/31/underwater-data-centres-are-coming-can-they-slash-co2-emissions-and-make-the-internet-fast>) and owes to the discussion in <https://earth.org/underwater-data-centres/>.

However, underwater data centers are utilized and deployed in a submarine environment and co-exist with other applications. These applications pose threat to the underwater data center. An example of an important application is the case associated with submarine ballistic missiles (Johnson 2023; Ellison et al. 2023; Kirchberger 2023; Kristensen et al. 2023). Johnson (2023) notes an increasing development and deployment of submarine launched ballistic missile systems such as the W76–2. The W76–2 is a modified version of the existing W76–1. The discussion in Johnson (2023) notes an increased development, and deployment of submarine launched ballistic missile systems. The Russia planned Poseidon; a deep diving unmanned nuclear armed underwater delivery vehicle is recognized in Fink (2023).

Ellison et al. (2023) recognize the need to develop suitable environments for sub-surface ballistic nuclear missiles. The research in Ellison et al. (2023) recognizes the case of the sub-surface ballistic nuclear missile as an extreme environment. It focuses on designing a friendly environment for the sub-surface ballistic missile nuclear submarine. This direction demonstrates that the viability of the technology required to enable the functionality of the sub-surface ballistic missile nuclear submarine (Arbatov 2020). The discussion by Kirchberger (2023) like (Ellison et al. 2023) recognizes the increasing use of submarine launched missile submarines. The discussion in Kirchberger (2023) considers the usefulness of submarine and ocean sub-surface-based missile systems in a weapons diversity strategy. In this case, the use of the submarine-based missile systems alongside land based and air-based defense systems is considered to deliver a robust defense system.

Kuhn in Kristensen et al. (2023) address an important non-technological aspect of submarine and ocean subsurface missile weapon systems. The discussion in Kristensen et al. (2023) notes an increasing proliferation of missile weapons development and nuclear arms terminology. However, the influence of the increasing technological advances and use of submarine-based missiles on important applications such as the underwater data center is important. This is important as more organizations adopt underwater data centers due to their low operational cost benefits.

A feasible solution is for defense authorities to provide information on the location of missile bearing deep diving submarine systems. However, the exposure of the concerned data contravenes the covert protocol underlying defense assets in the case of submarine missions. The use of deep diving submarine in missile system is designed in Johnson (2023). The use of deep diving submarine for missile launch in the future is beneficial due to the inherent covert benefits. However, the influence of advances in deep diving submarine-based missile alongside underwater data center functionality is yet to receive research consideration.

This section recognizes the emergence of underwater data centers as having low operational costs because they benefit from free ocean cooling (<https://news.microsoft.com/innovation-stories/project-natick-underwater-data-center/>; <https://earth.org/underwater-data-centres/>; Cutler et al. 2017; Hu et al. 2022; <https://spectrum.ieee.org/want-an-energyefficient-data-center-build-it-underwater>; <https://www.euronews.com/next/2022/08/31/underwater-data-centres-are-coming-can-they-slash-co2-emissions-and-make-the-internet-fast>). Being deployed in the underwater environment, underwater data centers share ocean resources with other underwater based applications. Some of these applications have known harmful effects on underwater data centers.

An important application that is recognized in this regard is the submarine hosting nuclear missiles intended for covert military operations. Submarines play a key role in military and defense application and have an advancing technology (Johnson 2023; Ellison et al. 2023; Kirchberger 2023; Kristensen et al. 2023; Fink 2023; Arbatov 2020). Being intended for civilian applications, underwater data centers have not been designed and placed in the ocean for military or defense applications. Hence, the use of underwater data centers in future networks has not considered the presence of defense submarines during missile launch. This is a challenge that needs to be addressed as missile paths are planned independently of submarine location.

2.2 Survivable networks and underwater data centers in future networks

Advances in nuclear technologies pose a significant threat to communication networks. The design of packet switching has been necessitated due to advances in nuclear technologies and weapons (Abbate 1999; Leslie 2013; Bay 2017; Clark et al. 2023). Leslie (2013) recognizes that realizing a survivable network in the event of a nuclear attack motivated packet switching. The focus in Leslie (2013) is on clarifying that the motivation to design the internet was driven by the need to realize a network that can survive a nuclear attack. Nevertheless, it is recognized

that the paradigm of packet switching as proposed is suitable for realizing a survivable network.

Bay (2017) discusses the underlying motivation behind survivable networks. In contrast to Leslie (2013), the discussion in Bay (2017) presents an holistic technical perspective. Furthermore, the discussion in Bay (2017) notes that artificial intelligence played a key role in the design of packet switching. The insight on the choice of a distributed system is linked to arise from motivation in biological neurons and artificial intelligence.

Clark et al. (2023) point out that packet switching provides a platform enabling the design of future user value-laden applications. The position in Clark et al. (2023) is that the use of packet switching addresses the challenges of ensuring network survivability due to nuclear attacks. However, the internet has evolved due to the incorporation of cloud computing and networked data centers. Data centers play a key role on the internet and its evolution as seen in Ensan et al. (2021), Kliks et al. (2017), Lingshu et al. (2021).

The increased use of data centers in future networks makes them a key component of the emerging internet. Data centers comprise networked servers that enable information storage, process, access, and transfer. They can be attacked by rogue actors because of their critical role in the future internet. Moreover, the use of underwater data centers was not considered in Ensan et al. (2021), Kliks et al. (2017), Lingshu et al. (2021) and Abbate (1999), Leslie (2013), Bay (2017), Clark et al. (2023). However, there are advances in underwater technologies as seen in submarine launched ballistic missiles (Peters 2021; Clark 2023; Zhao 2022).

The notion of an arms race in the case of submarine systems and the associated launched missiles is recognized in Zhao (2022). Hence, the previous threat to communication networks observed in Abbate (1999), Leslie 2013, Bay (2017) reoccurs. The re-occurrence arises in between underwater data centers and deep diving submarines with missile payload.

Grossi (2022) notes that the international atomic energy agency (IAEA) provides laws and protocols for safe use of nuclear technology. The discussion in Grossi (2022) observes that the IAEA ensures that the diversion of nuclear material to produce nuclear weapons does not occur. A similar perspective can be found in Lanin (2023). The discussion in Hiroshima for Global Peace Plan (2018) notes an increasing reluctance of nuclear weapon states to disarm. In addition, the increasing interest of modernizing nuclear arsenals by nuclear weapon states is also observed. Furthermore, increasing nuclear arming by new states is also observed. From Hiroshima for Global Peace Plan (2018), Ruff (2022), the damaging effect of nuclear

weapons and nuclear threat still require consideration in modern society.

The IAEA plays a significant role in ensuring the non-transfer of nuclear technology into weapon purposes. It regulates the usage of nuclear technology and ensures its use for peaceful purposes such as power generation and medical applications. Furthermore, a peaceful use of nuclear technology is the provisioning of power for submarine systems. This can be seen in the US's Columbia class of naval submarines intended to replace the aging and outgoing Ohio class submarines (Congressional Research Office 2022; van Hooft 2020; Columbia-class/default.asp). In addition, there are advances on the use of submarine with modern missiles. Such modern missile improvement could involve the addition of nuclear warhead payload. Existing research focusing on missile modernization are being increasingly made by other nations (Abbasi et al. 2023; Kristensen et al. 2023; Gale and Hochhaus 2023; Kristensen and Korda 2019). The IAEA supports the peaceful use of nuclear power in enabling the operation of either military submarine systems. From this perspective, the use of nuclear energy technology for enabling the operation of underwater computing platforms is allowed. This is because the application context is peaceful. However, the IAEA has not explicitly considered the applications of nuclear technology with relation to underwater computing platforms. In addition, the IAEA's outlook focuses on the relations between potential multiple applications of nuclear technology. However, the context of underwater data centers should receive research consideration from the perspective of enabling future nuclear co-existence.

The discussion in this section recognizes the emergence of underwater data centers as a future data center system. It is recognized that the need to design survivable communications network motivated the design of the packet switching communication systems. The discussion recognized that there is a significant interest in nuclear technology in the directions of weaponization and peaceful uses (regulated by the IAEA).

An identified drawback is that the use of underwater data centers has not considered that the underwater environment is a missile focused war theatre. Hence, the activity associated with submarines with missile payloads and the threat posed to underwater data centers is yet to receive consideration. However, this threat is considered a significant disruption effect.

The existing research that has been discussed identifies that the advances in nuclear weapons technology motivate the development of survivable communication networks. However, the context of survivable communication networks that has received consideration has not recognized the underwater data center. The previously existing

survivable network comprising underwater data centers is affected by missiles. The concerned missiles are launched from multiple submarines and damage underwater data centers. Such a scenario is feasible as the underwater data centers have not been widely adopted. In such a case, packet transmission from underwater data centers in the underwater environment becomes infeasible.

A summary of the existing research that has been considered is presented in Table 1. The discussion in Table 1 is presented with an underlying background. The background is that the development of defense submarines does not consider the deployment of underwater data centers. Hence, the focus of Table 1 is the description of existing research that has focused on underwater data centers.

The discussion in this section shows that existing research recognizes the increasing consideration for the use of nuclear weapons in defence applications. The increasing use of nuclear weapons is recognized in Peters (2021), Clark (2023), Zhao (2022) to constitute a threat to other underwater based applications. The internet is an important underwater based application. The internet benefits from a considerable number of different technologies. An important potential technology that can enhance internet access is the underwater data center. Advances in nuclear technologies has been recognized to pose a threat to the internet as seen in Abbate (1999), Leslie 2013, Bay (2017). The development and deployment of underwater data centers in the future internet have arisen from the need to reduce operational costs. The development of underwater data centers have not received consideration alongside development in nuclear weapons noted in Zhao (2022). Nevertheless, both applications i.e., underwater data center, and defense submarines use the underwater environment. Therefore, it is important to design a mechanism and system architecture to ensure that these applications do not pose performance challenges to each other.

3 Problem description

The challenge being addressed is described in this section. The discussion in this section has two aspects. The first aspect discusses the network context being considered. The second aspect presents the attack scenario.

3.1 Network context

The considered scenario is one in which there are multiple underwater data centers that belong to different computing service providers. Each underwater data center comprises multiple servers that are in a pod. In addition, underwater data centers enable data transfer with external entities and networks. This is done via fiber optic cables. The

Table 1 Existing Research on the Development, and Deployment of Underwater Data Centers

S/ N	Existing work	Strengths	Aspects for future contribution
1	Cutler et al. (2017)	The discussion presents the functional analysis of underwater data centers. The discussion recognizes that underwater data centers have a reduced failure rate in comparison to existing terrestrial data centers	A multi-event failure analysis is required to consider other types of events that can lead to a potential underwater data center failure. In addition, a solution to address the different types of failures besides those arising from computing and power system failure are required
2	Hu et al. (2022)	The presented research addresses the challenge of installing servers in underwater data centers. The solution being proposed aims to achieve the packing of servers in an efficient manner aboard underwater data centers	Additional research on studying how the scalability of the presented research influences large sized underwater data centers requires further consideration
3	Roach (2020) (https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter/)	An enterprise perspective of an in-field performance of the underwater data center is presented. The enterprise underwater data center that receives focus is that of the Microsoft Project Natick	Aspects requiring further consideration is the integration of the underwater data center into a communication network
4	Earth.org (2020) (https://earth.org/underwater-data-centres/)	The discussion focuses on the rationale for the choice of Orkney as a deployment site for the Microsoft Data Center, Project Natick	Additional analysis of the performance benefits of the cooling tower and presentation of the result is required
5	Gallagher (2022) (https://www.euronews.com/next/2022/08/31/underwater-data-centres-are-coming-can-they-slash-co2-emissions-and-make-the-internet-fast)	The focus is on the performance and environmental benefits of the Subsea cloud enterprise underwater data center. The presented underwater data center developed by Subsea cloud is low cost	Further aspects as regards the scalable deployment of the low-cost underwater data center requires further consideration

underwater data centers are in a region with low temperature having access to a high volume of cold ocean water. This enables the realization of free ocean water cooling. Furthermore, the underwater data centers are separated from each other by at least 1 km. The underwater data centers in this case provide connectivity and computing services to a connection of separated coastal areas with high population of internet and network subscribers. The scenario being considered is shown in Fig. 1.

In Fig. 1, each underwater data center is connected to a shore–gateway via a fiber optic cable. Each of the cities i.e., City 1, City 2 and City 3 is connected to underwater data centers via the shore–gateway. The maximum ocean depth in this case is denoted as $h_{\max}^{udc}$. The scenario in Fig. 1 does not show the presence of deep diving submarines that host missile systems. The underwater data centers are located at an altitude above the altitude of deep diving submarine systems. In this case, deep diving submarine systems are located at a greater ocean depth being intended for covert ocean operations. The siting and deployment at greater ocean depths is deemed necessary for the realization of covert mission maneuvers and operations. The

influence of the deep diving submarine systems with launched missiles is shown in Fig. 2.

The scenario in Fig. 2 shows three deep diving submarine systems i.e., DSS 1, DSS 2, and DSS 3. Each of the deep diving submarine systems launch missiles targeting each city. The launched missiles traverse paths on the locations hosting underwater data centers. The underwater data centers are immobile and cannot avoid the collision resulting from the launched missile. In Fig. 2, the maximum deep diving submarine depth is denoted $h_{\max}^{dss}$ such that $h_{\max}^{dss} > h_{\max}^{udc}$. DSS 1 causes a loss of functionality regarding underwater data centers 2 and 3. The launch of missile from DSS 3 causes a loss of functionality regarding underwater data center 1 indicated as UDC 1 in Fig. 2.

The relations in Fig. 1 show the network architecture with a focus on the underwater data centers i.e., UDC 1, UDC 2, UDC 3, and UDC 4. The scenario presented in the case of Fig. 1 does not show the threat arising from the deep diving submarine systems. Instead, the scenario in this case is one in which the underwater data centers are deployed in a maritime resource where no defense applications or systems are present. The case where the

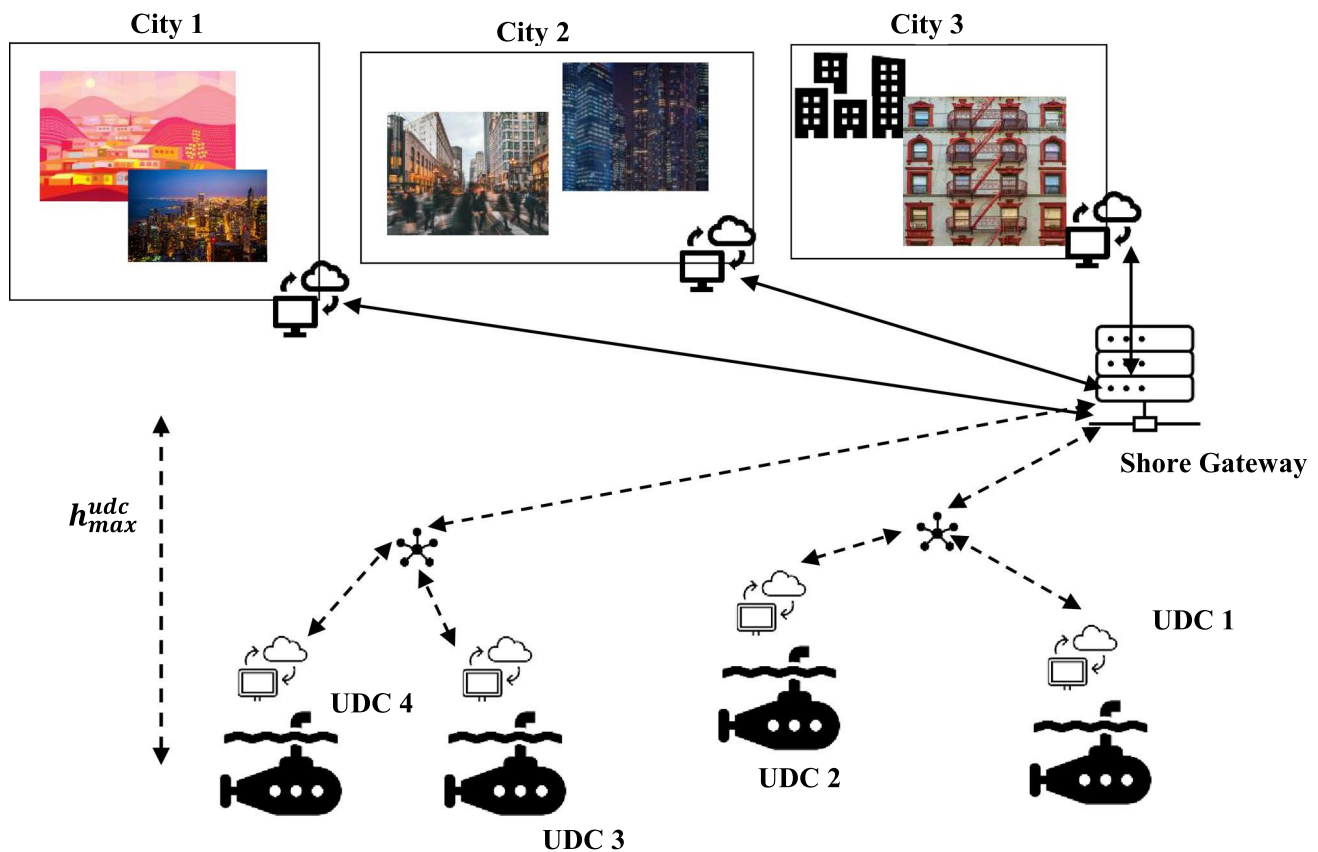


Fig. 1 Network Scenario showing relations between underwater data centers, UDC 1, UDC 2, UDC 3, and UDC 4 and the shore-based gateway. In this case, there are no deep diving submarines or defense applications in the concerned maritime resource

underwater data centers are affected by defense applications is shown in Fig. 2.

The scenario in Fig. 2 is one in which deep diving submarine systems and defense applications are in the concerned maritime resource. The deep diving submarine systems are deployed in a manner to achieve covert operations. In addition, the deep diving submarine systems are deployed at a greater ocean depth than the underwater data centers. In the scenario in Fig. 2, there are three deep diving submarine systems i.e., DSS 1, DSS 2, and DSS 3.

3.2 Attack scenario

The scenario in Figs. 1 and 2 comprises multiple underwater data centers and deep diving submarine systems. The discussion in this aspect presents a formulation of the attack scenario. It considers that underwater data centers and deep diving submarine systems host entities. In this consideration, the underwater data center experiences a collision. The collision arises between the underwater data center and a missile launched from an active submarine having missile weapon payload. Furthermore, an active underwater data center can also be in a state where it does

not experience collision with a launched missile. In modelling the attack scenario, the underwater data center is an active node in a communication network. This also applies to the missile bearing deep diving submarine system.

Let α and β be the set of underwater data centers and deep diving submarine systems (bearing missiles), respectively.

$$\alpha = \{\alpha_1, \alpha_2, \dots, \alpha_A\} \quad (1)$$

$$\beta = \{\beta_1, \beta_2, \dots, \beta_B\}, \quad (2)$$

where A and B are the total number of underwater data centers and missile bearing deep diving submarine systems, respectively.

The b^{th} deep diving submarine system, $\beta_b, \beta_b \in \beta$ comprise multiple missiles such that:

$$\beta_b = \{\beta_b^1, \beta_b^2, \dots, \beta_b^M\}. \quad (3)$$

where M is the total number of missiles aboard the b^{th} deep diving submarine system, β_b .

Let $I(\alpha_a, \beta_b^m, t_y) \in \{0, 1\}$, $\alpha_a \in \alpha$, $\beta_b^m \in \beta$ signify the collision status between α_a and β_b^m at the epoch t_y . The attack from the missile β_b^m collides with the underwater data center α_a

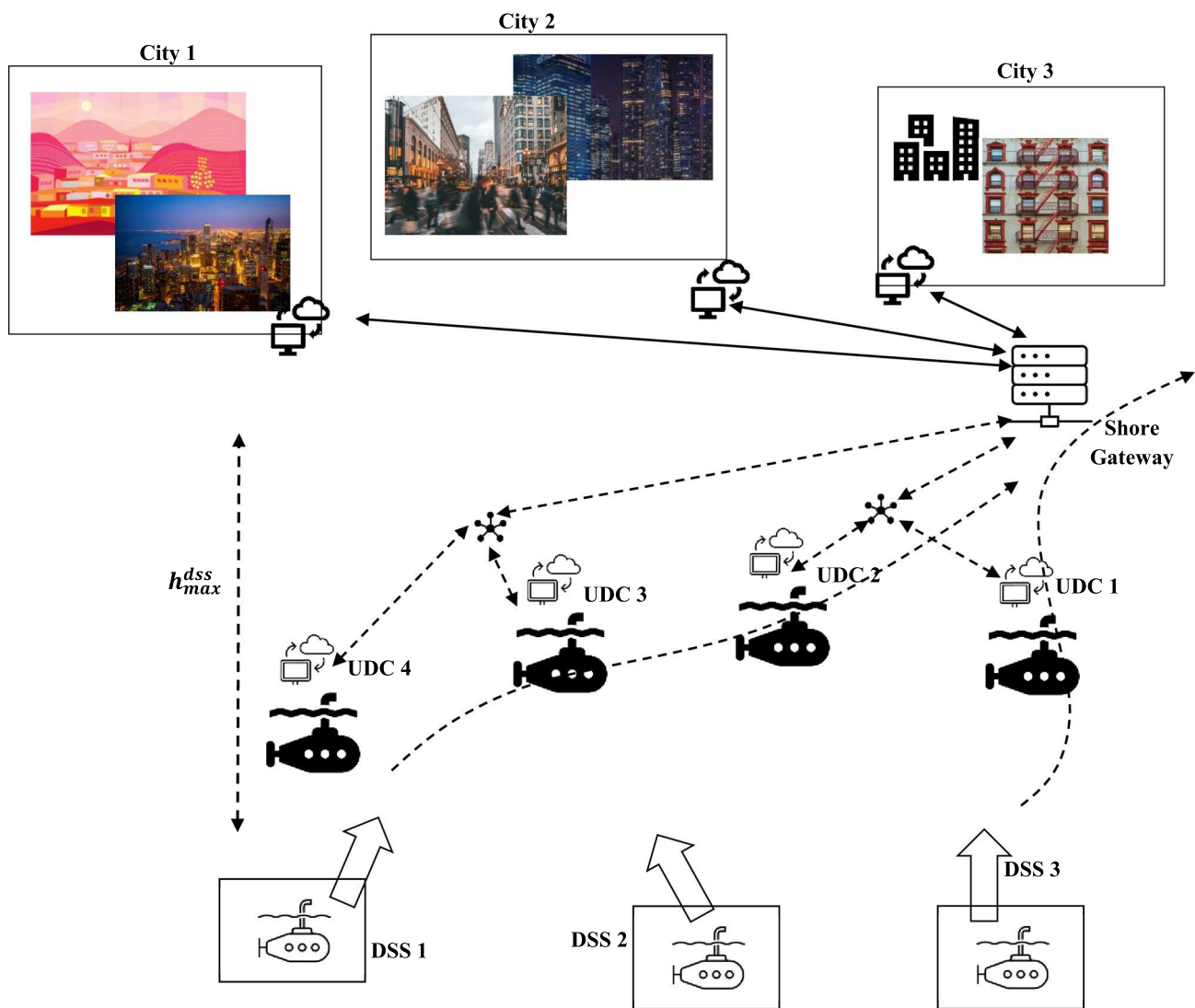


Fig. 2 Scenario showing relations between underwater data centers UDC 1, UDC 2, UDC 3, and UDC 4 and shore-gateway considering threats from deep diving submarine systems

and prevents its continued functionality of α_a at the epoch t_y when $I(\alpha_a, \beta_b^m, t_y) = 1$. An attack from the missile β_b^m does not collide with the underwater data center α_a and there is no service discontinuity for the underwater data center α_a at the epoch t_y when $I(\alpha_a, \beta_b^m, t_y) = 0$.

The attack from the missile β_b^m causes the non-functioning of multiple smart cities via the disruption of the underwater data centers α_a and α_{a+1} , $\alpha_{a+1} \in \alpha$ at the epoch t_y when $I(\alpha_a, \beta_b^m, t_y) = 1$ and $I(\alpha_{a+1}, \beta_b^m, t_y) = 1$.

A feasible attack from the missile aboard the deep diving submarine system can be described by:

$$\{I(\alpha_a, \beta_b^m, t_y), I(\alpha_{a+1}, \beta_b^m, t_y), \dots, I(\alpha_{a+q}, \beta_b^m, t_y)\} = \{1, 1, \dots, 1\} \quad (4)$$

$$\{I(\alpha_a, \beta_b^{m+1}, t_y), I(\alpha_{a+1}, \beta_b^{m+1}, t_y), \dots, I(\alpha_{a+q}, \beta_b^{m+1}, t_y)\} = \{0, 0, \dots, 0\}, \alpha_{a+q} \in \alpha, \beta_b^{m+1} \in \beta \quad (5)$$

$$\{I(\alpha_a, \beta_b^{m+1}, t_{y+1}), I(\alpha_{a+1}, \beta_b^{m+1}, t_{y+1}), \dots, I(\alpha_{a+q}, \beta_b^{m+1}, t_{y+1})\} = \{1, 1, \dots, 1\}, \alpha_{a+q} \in \alpha, t_{y+1} \in t \quad (6)$$

The case in (4) is one in which the attack from the missile β_b^m causes a damage to underwater data centers α_a, α_{a+1} and α_{a+q} , $\alpha_{a+q} \in \alpha$ at the epoch t_y . In this case, the attack from the missile causes a damage to the underwater data center. This is because the indicator variable describing the collision status has a value of one at all epochs. The damage to the underwater data center causes a loss of service continuity.

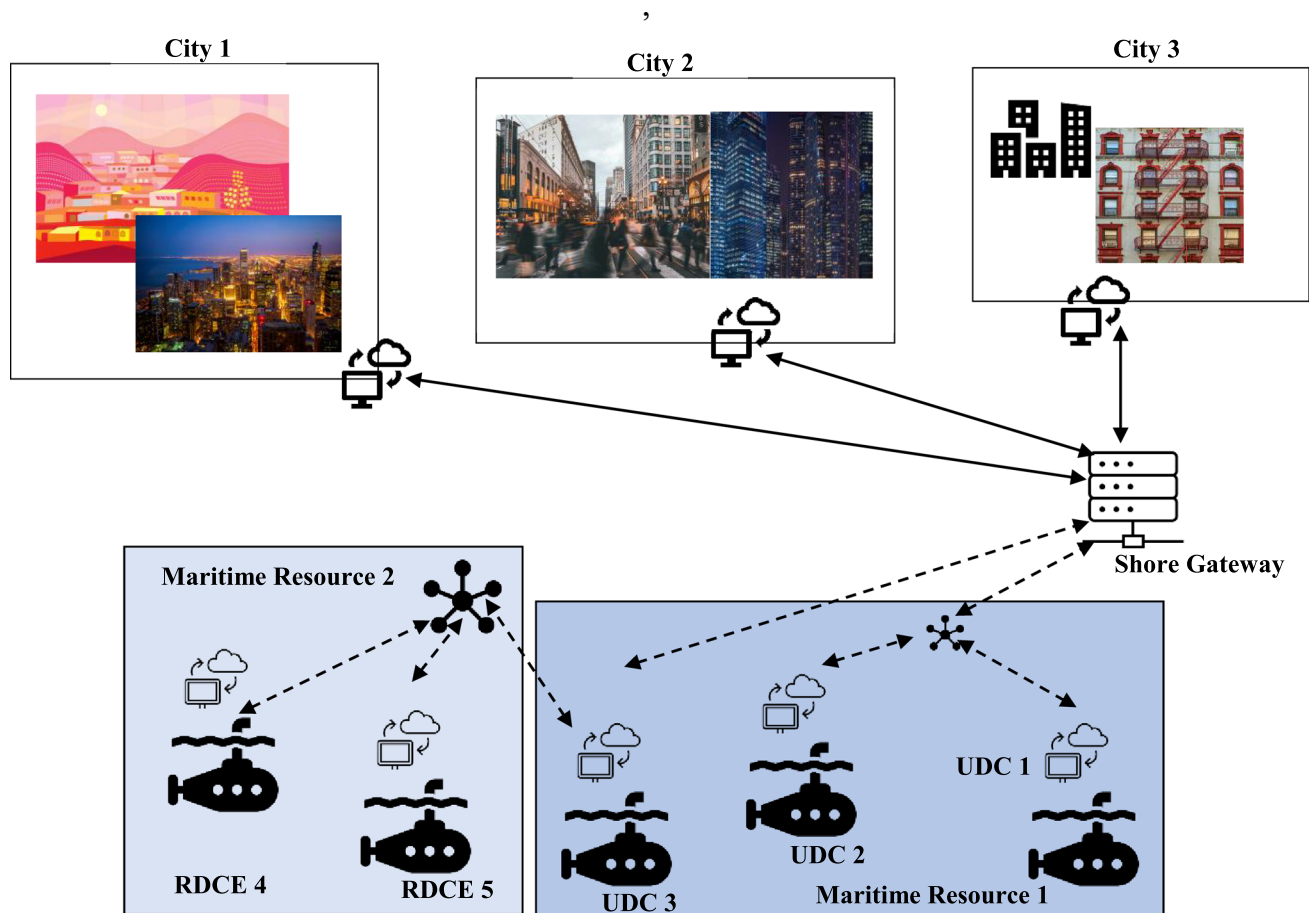


Fig. 3 Network scenario showing the incorporation of redundant data center entities as envisaged in the proposed network architecture

In (5), the attack from the missile $\beta_b^{m+1}, \beta_b^{m+1} \in \beta$ does not cause a damage to the underwater data centers α_a, α_{a+1} and $\alpha_{a+q}, \alpha_{a+q} \in \alpha$ at the epochs $t_y, t_y \in t$ as the indicator variables. This indicator variable describes the collision status and has a value of zero at all epochs. This is because the missile β_b^{m+1} has not been launched. Hence, the values of all instantaneous indicator variables are zero.

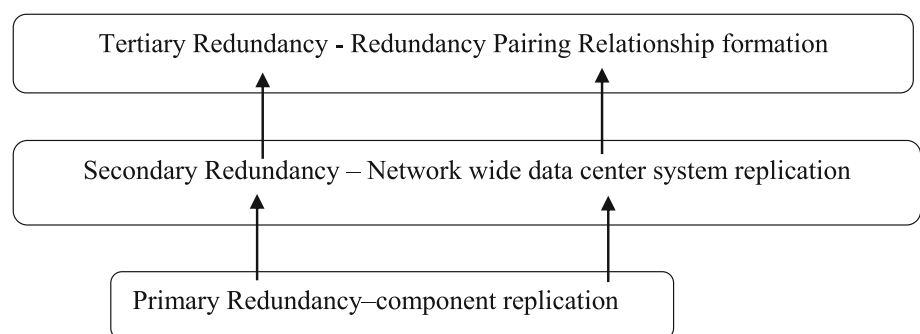
The case in (6) considers the impact of missile β_b^{m+1} at the epoch $t_{y+1}, t_{y+1} \in t$. In the considered scenario, the missile

attack results in a damage to the underwater data centers α_a, α_{a+1} and α_{a+q} .

Furthermore, underwater data centers damaged in (4) are replaced in (5) after service disruption. The replaced underwater data centers are damaged by missiles launch again in (6). It is important to prevent loss of service disruption due to underwater data center damage. The resulting damage arises when the coastal locations have a missile defense system.

Therefore, it is important to design a mechanism ensuring a non-loss of underwater data center

Fig. 4 Multi-Tier Redundancy showing the relations between the redundancy tiers in the proposed architecture



functionality. The mechanism arises the service disruption due to the missile attack observed in the scenarios presented in (4) and (6) at different epochs.

4 Proposed mechanism and network architecture

The proposed network architecture incorporating redundancy and enabling the realization of network survivability. In this case, the network incorporating underwater data centers is presented in this section. The discussion has two parts. The first part describes the proposed network architecture wherein a underwater data center has an associated data center system. The novelty of the proposed network architecture lies in the design of a network enabling the continuity of cloud functionality. The concerned subscribers were previously anchored to underwater data centers when nuclear missile attacks occur. The second part presents the proposed nuclear co-existence protocol. The co-existence protocol enables underwater data centers to share ocean location resources with submarine launched missiles. The location resource sharing enhances the survivability of underwater data centers. The network survivability arises as the launch of submarines is no longer independent of the existence of underwater data centers.

4.1 Data center future networks incorporating redundancy

The discussion in this section presents a framework enabling other data centers to continue service delivery when underwater data centers experience service disruption. The disruption arises due to the attack from missiles

launched from deep diving submarine systems. The considered scenario is described in the transitions discussed in (4), (5) and (6). The discussion presents a network architecture that enables subscribers have continued access to cloud functionality. The framework being presented incorporates redundancy.

In the proposed redundancy framework, an underwater data center has associated redundant data centers in other locations. The candidate redundant data centers are other underwater data centers, terrestrial data centers and stratosphere data centers. The redundant underwater data center is in another maritime resource (ocean and underwater environment). Redundant data centers can also be in the terrestrial or stratosphere environment. An underwater data center is connected to a shore-based gateway (shore-gateway). The shore-gateway is connected to the entity enabling data transfer to the identified redundancy data center entities. The entity that communicates with the redundant data center entity is the redundancy gateway. The redundancy gateway is connected to the shore-gateway. However, the shore-gateway enables the underwater data centers to have a connectivity to external networks besides the redundant data center entities. The redundancy gateway provides underwater data center– redundant data center entity connectivity.

Initially, redundant data center entities are realized via a direct replication of data center capability. The replication involves a launch and use of a new data center in the terrestrial and non-terrestrial environment. The relations between the terrestrial and non-terrestrial data centers are shown in Fig. 3. The relations in Fig. 3 shows the relations between the underwater data centers, underwater data center 1, underwater data center 2 and underwater data center 3, and associated redundant data centers, RDCE 1,

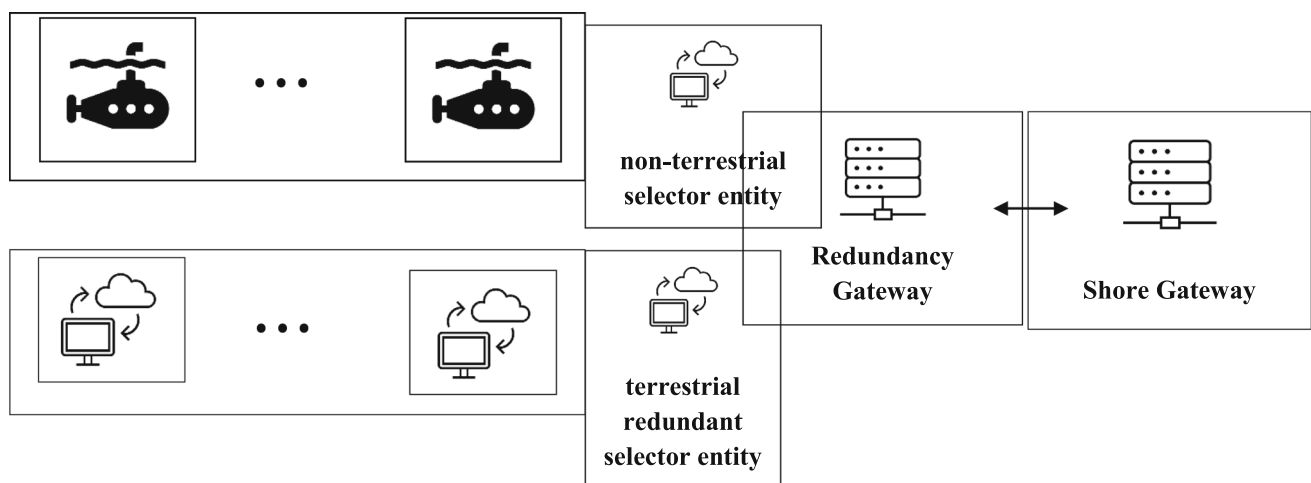


Fig. 5 Relations between the redundancy gateway, shore-gateway, non-terrestrial selector entity and terrestrial redundant selector entity enabling the acquisition of data in the proposed network architecture

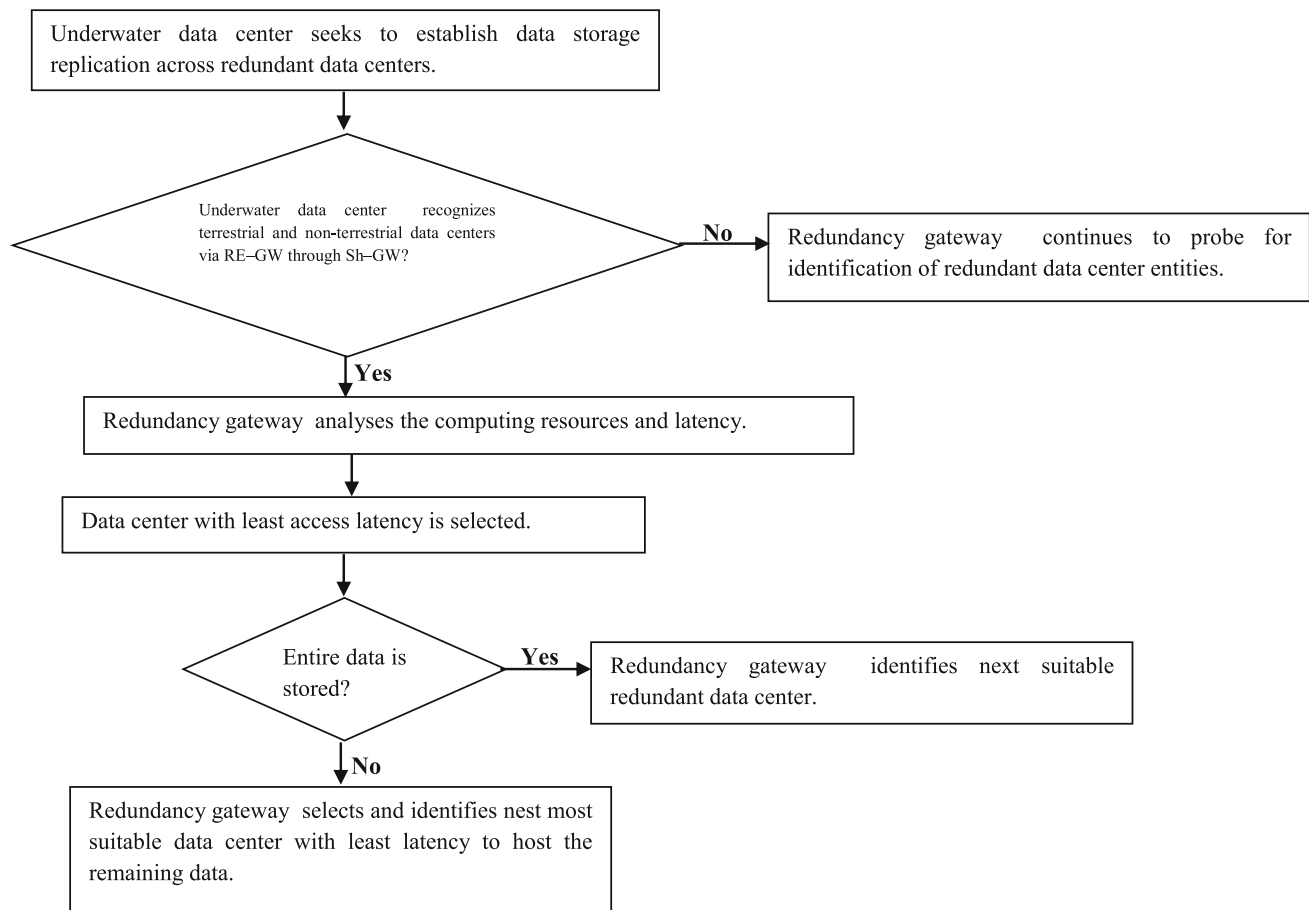


Fig. 6 Flowchart describing steps arising from the proposed mechanism and network architecture

RDCE 2, RDCE 3, RDCE 4 and RDCE 5. The shore-gateway enables the connection of the redundancy-gateway, underwater data center 1, underwater data center 2, and underwater data center 3 to external cloud networks. The shore-gateway is connected to the redundancy gateway via high-speed links. The redundancy-gateway is connected to the redundant data centers RDCE 1, RDCE 2, RDCE 3, RDCE 4 and RDCE 5. In Fig. 3, the underwater data centers and redundant data center entities are in different maritime resources. The underwater data centers and redundant data center entities are in maritime resource 1, and maritime resource 2, respectively.

The data center incorporates redundancy at three levels i.e., primary redundancy, secondary redundancy, and tertiary redundancy. Primary redundancy refers to the implementation of component level 1 function replication in each data center. This is applicable to underwater data centers, terrestrial data centers or stratosphere-based data centers. Secondary redundancy is associated with the replication of data center functionalities via the use of redundant data center entities. Tertiary redundancy concerns the identification and selection of an redundant data

center entity as the redundant data center for a given underwater data center. In this case, the tertiary redundancy targets the realization of a redundant pair. The relations between the primary redundancy, secondary redundancy and tertiary redundancy are presented in Fig. 4. The redundancy pairing relationships enables the realization of underwater data center–redundant data center pair. The redundancy pairing is executed by the redundancy gateway.

The concerned computing entity utilizes information on the: (1) Operational power usage effectiveness, (2) idle computing resources, (3) mean throughput (link speed) associated with data access, (4) mean latency (delay) associated with data access and (5) operational costs. A suitable target redundant data center has a low operational cost, operational power usage effectiveness, and mean latency. The target redundant data center has a high value for the: (1) idle computing storage, (2) available computing resources and (3) mean throughput (link speed). These parameters are observed from the set of reachable data centers from the redundancy gateway. The redundancy gateway hosts ground station and fiber optic connections

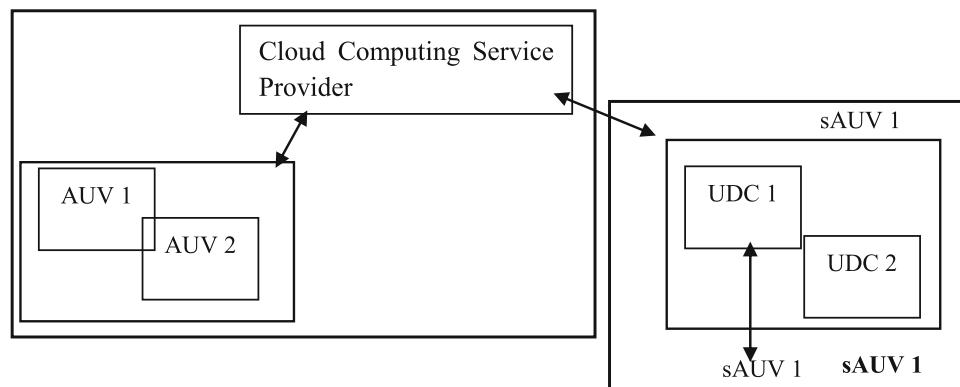


Fig. 7 Relations between the pre-underwater data center deployment phase and underwater data center deployment phase showing comprising entities. The entities are the support autonomous underwater vehicle 1 (sAUV 1), autonomous underwater vehicle (AUV 1),

autonomous underwater vehicle (AUV 2), underwater data center 1 (UDC 1), underwater data center 2 (UDC 2), and support autonomous underwater vehicle 2 (sAUV 2)

for reaching redundant terrestrial, stratosphere, and underwater data centers. The identifier of the underwater and redundant data centers are the outputs of the tertiary redundancy pairing process. The aspect of the secondary redundancy focuses on replicating the entire data center functionality. The replication involves sharing of the data to prevent loss in the event of a underwater data center permanent damage to a nuclear missile attack.

It is important to consider the case where the underwater data centers establish redundancy relationships with terrestrial and stratosphere-based data centers. In this case, the role of the redundancy gateway changes as most redundant data center entities are in the terrestrial environment. This is because of the low adoption of stratosphere and underwater data centers in comparison to terrestrial data centers. The redundancy gateway maintains connection with terrestrial data centers. The residual computing resources and network performance determine the suitability of a terrestrial data center.

A similar set of parameters are considered for stratosphere data centers and underwater data centers. The redundancy gateway incorporates entities enabling the choice of data centers. The considered data centers are existing terrestrial data centers, available stratosphere-based data centers and underwater data centers. The redundancy gateway comprises two entities that select the data center. These entities are the terrestrial redundant selector entity and the non-terrestrial redundant selector entity. The role of the terrestrial redundant selector entity and non-terrestrial selector entity is shown in Fig. 5.

In Fig. 5, the redundancy gateway selects a redundant data center using information from the terrestrial redundant selector and non-terrestrial selector entities. The terrestrial redundant selector entity hosts information on: (1) Available computing resources, (2) Available data storage capacity, and (3) Mean network parameters (link speed and

latency). Similar information is obtained for the underwater data center and stratosphere data center. The architecture in Fig. 5 enables the identification and selection of suitable data centers in the redundancy pairing relationship.

The data from a given underwater data center can be replicated across multiple data centers in each storage redundant relationship. This is because the concerned data centers have various levels of computing resource utilization. However, the latency associated with data upload and download does not exceed a certain and pre-determined threshold latency. The selection of the redundant data center is shown in the flowchart in Fig. 6. The flowchart in Fig. 6 considers the realization of low latency in accessing and transferring the concerned data being replicated. The low latency requirement is deemed necessary to meet the ultra-low latency requirements being expected of future communication networks. If a suitable redundant data center is not recognized, the redundancy gateway continues to search for redundant data center candidates. The functionality is terminated when suitable redundant data center entities are identified. The storage of data from the underwater data center can also occur across multiple redundant data center with highest speed links. The data storage occurs alongside a significant amount of data storage resources is selected for data replication and associated storage. The network architecture has a limited survivability because the shore-gateway and redundancy gateway entities are not centralized.

The discussion in Bay (2017) notes that artificial intelligence has influenced the choice of a distributed system for the implementation of a packet switching system. Hence, the entities described in the shore-gateway and redundancy gateway should be distributed and not centralized. In realizing a distributed functionality for the redundancy gateway and shore-gateway, the research proposes the distributed gateway approach.

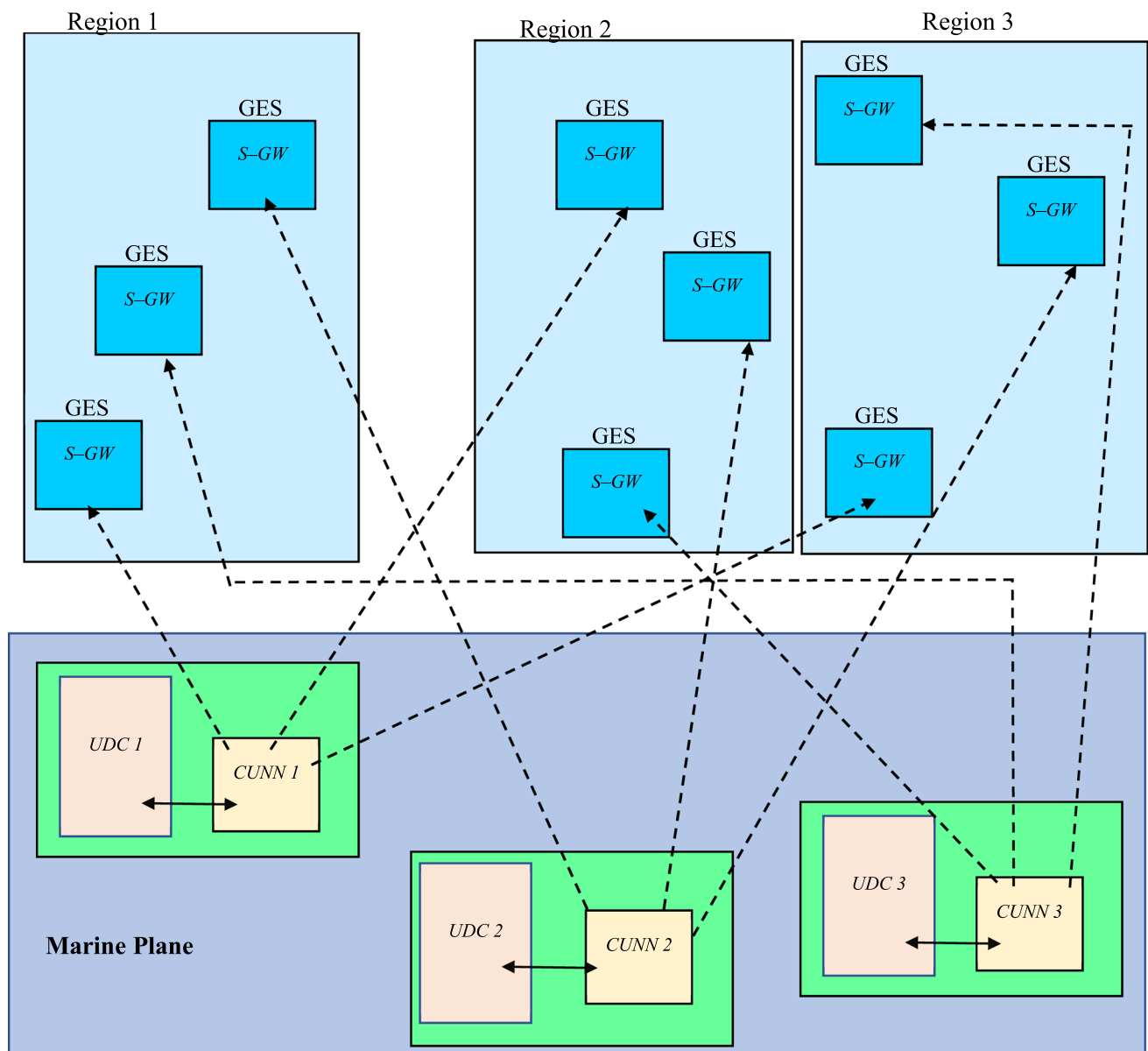


Fig. 8 Diversity enabling the critical underwater network node attachment to multiple survival gateways in a diversity aimed at surviving a nuclear attack. The concerned network entities are

gateway earth station, underwater data centers UDC 1, UDC 2, UDC 3; critical underwater network nodes CUNN 1, CUNN 2, and CUNN 3; and the survival gateway (S – GW)

In the distributed gateway, the functionalities of the shore–gateway and redundancy gateway are in a single gateway i.e., the survival gateway. Each underwater data center is connected to a different survival gateway. The network architecture in this case integrates the functionalities that were previously considered separate. The robustness of the network architecture is improved by introducing multiple integration points in the terrestrial segment and underwater segment. These integration points enable the realization of connectivity to multiple underwater data centers. In the terrestrial segment, the integration points merge the function of the shore–gateway and

redundancy gateway in the distributed gateway. Each underwater data center has multiple connections to the underwater integration point. The underwater integration point is linked to the multiple terrestrial integration point.

4.2 Underwater data centers: nuclear co-existence protocol

The discussion here presents a co-existence protocol for weapon payload bearing submarine systems and underwater data centers. In this case, the resource being shared is ocean space. The weapon payload bearing submarine

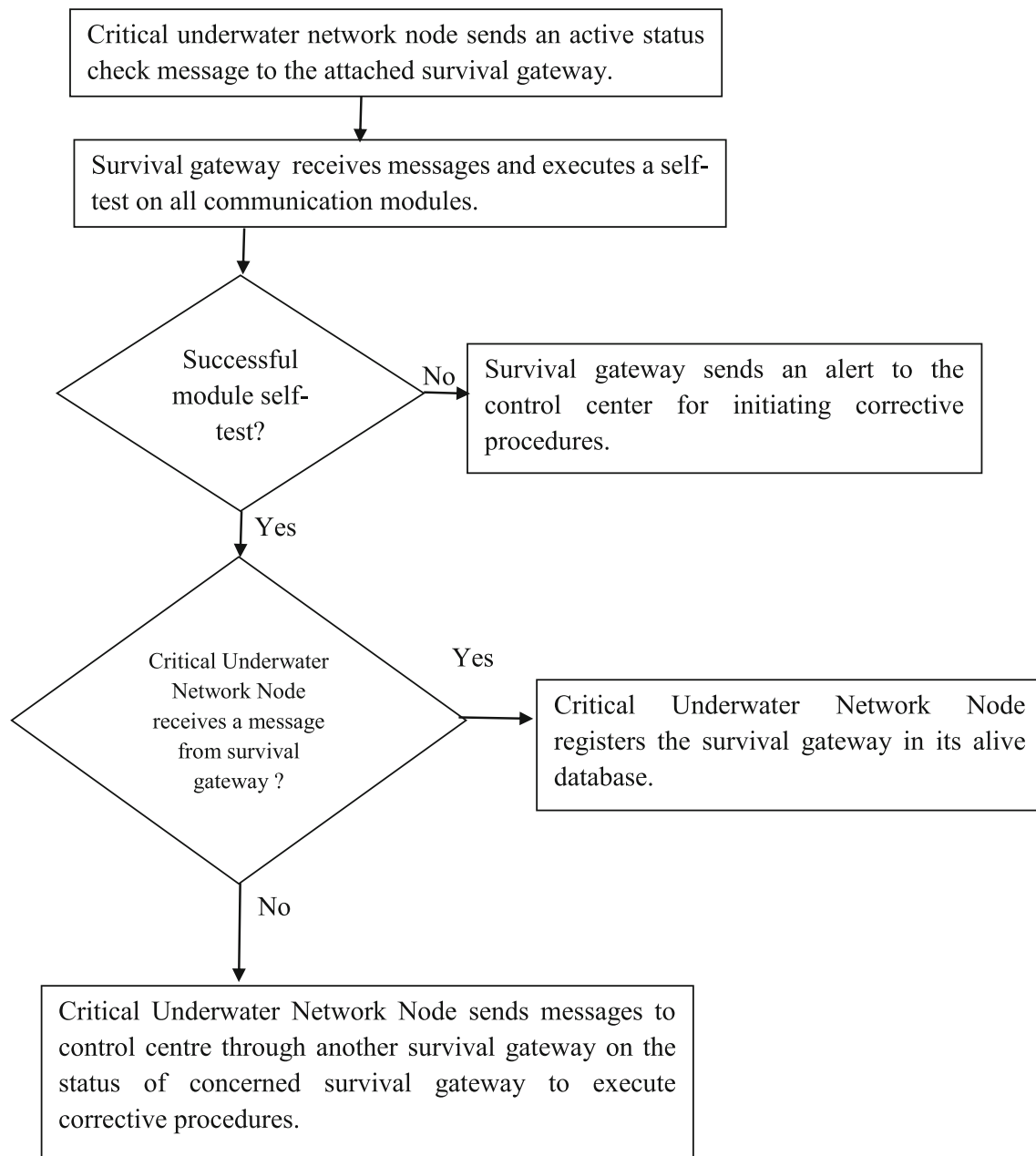


Fig. 9 Flowchart showing tasks being executed in the proposed diversity approach associated with the proposed network architecture

systems and underwater data centers are at different ocean depths. In addition, deep diving weapon payload bearing submarine systems have underwater paths for the launched missile. The challenge here arises when the launched missile path intersects with the underwater data center's ocean sub-surface location. It is important to consider that the ocean is a dynamic environment with a variable hydrodynamic friction. In the underwater data centers, the important parameter is the low temperature of the ocean water making it cold and suitable for free cooling purposes. Therefore, co-existence can be realized by siting the weapon payload bearing submarine systems in a path

where missile trajectory has the least underwater hydrodynamic friction. Such a path should also have a free coolant with sufficiently low temperature to realize low cooling. The detection of least hydrodynamic drag paths in the underwater environment is executed by the underwater data center in its pre-deployment phase. In the pre-underwater data center deployment phase, an autonomous hydrodynamic sensor is deployed. Such a sensor is feasible for use in the underwater environment as seen in Kristensen and Korda (2019), Lamberti et al. (2015), Uchida et al. (2019), Kazys et al. (2015). The sensor technologies in Kristensen and Korda (2019), Lamberti et al. (2015),

Uchida et al. (2019), Kazys et al. (2015) enable the measurement of water density. The density is considered as it is seen to influence the drag in each context as seen in (6) of Ridley et al. 2022.

In the pre-underwater data center deployment phase, an autonomous underwater vehicle is deployed by the entity desirous of deploying the underwater data center. This is done to determine the ocean's regions having a low density (potential paths for submarine launched missiles). These points are described using the data on the depth and distance from the reference ocean shore. Alternatively, the use of more robust underwater positioning systems such as (Won and Lee 2020) is suitable. The deployment of underwater data centers is done in two phases. The first phase is the pre-underwater data center deployment phase. The second phase is the underwater data center deployment phase. In the pre-underwater data center deployment phase, autonomous underwater vehicles detect the ocean's locations and regions having a low density. This is done with the aim of determining multiple locations through which lines of regular trajectory or irregular trajectory can traverse. These locations are held in the autonomous underwater vehicle onboard memory. In addition, the details of the locations as observed by the navigation technology in Won and Lee (2020). Relations between the pre-underwater data center deployment phase and underwater data center deployment phase is shown in Fig. 7.

In Fig. 7, the underwater data centers hosted within a given separating distance are attached to support autonomous underwater vehicles. Each support autonomous underwater vehicle executes the same function as the autonomous underwater vehicles. The observed density values obtained from support autonomous underwater vehicles are used to determine the suitability of the a given location. This is due to the dynamic nature of the submarine environment. In the case where an ocean location is unsuitable, it describes a potential path for missile launched from the weapon payload submarine system. In a case where this is true, the underwater data center location is changed. The location is changed given that there is long-term increase in the density of the ocean across multiple locations.

The proposed nuclear co-existence protocol enables the underwater data center to avoid being in the path of the launched missile. In this case, nuclear missiles fired from the submarine are aimed at a given direction and do not cover all feasible ocean regions concurrently. This is feasible due to the prohibitive costs of launching a high number of submarines to cover all ocean depths and orientation concurrently. Furthermore, it is challenging to

realize submarine systems with an infinite degree of freedom as regards missile launch paths. In the co-existence protocol, launched missiles do not cause the survival gateway to experience damage that leads to total service discontinuity. The damage is not applicable to the survival gateway that merges the functionality of the redundancy gateway and shore-gateway in a single entity. The entity is the distributed gateway. The underwater data center is connected to the survival gateway. The survival gateway is linked to an earth station enabling communications with terrestrial and the stratosphere-based data centers.

Each underwater data center is connected to multiple survival gateways. The survival-gateways are deployed along the ocean's coastline and connected to a critical underwater network node. The critical underwater network node is linked to a multiple survival gateway. The link to multiple survival gateways enables the realization of an architecture incorporating survival gateway diversity. The number of submarines and feasible firing positions is smaller than the number of survival gateways and critical underwater network nodes. Hence, the occurrence of a missile attack that leads to a loss of connectivity between the inter-data center networks does not cause network connectivity breakdown. This is because the survival gateway diversity enables the realization of a scenario where redundant survival gateways are present in the proposed architecture.

In addition, existing work in Periola (2020) demonstrates the design of mechanism enabling the prevention of the loss of functionality of network connectivity in stratosphere-based data centers. The stratosphere-based data centers being considered here incorporate this mechanism and avoid the loss of network connectivity due to missile attack.

The proposed survival gateway diversity architecture is shown in Fig. 8. The scenario in Fig. 8 is one in which there are three underwater data centers i.e., underwater data center 1, underwater data center 2 and underwater data center 3. Each underwater data center has its own critical underwater network node. The critical underwater network node associated with underwater data center 1, underwater data center 2, and underwater data center 3, are CUNN 1, CUNN 2, and CUNN 3, respectively. However, the diversity architecture can involve multiple survival gateways in multiple regions. In addition, there are three regions hosting survival gateway with each having a gateway earth station. The critical underwater network node is connected to three survival gateways with each survival gateway being in three regions. In addition, each critical underwater network node is connected to an sur-

Table 2 Simulation parameters for the three considered scenarios

S/N	Parameter	Value
Target Functional Duration—for Terrestrial, Stratosphere, and Underwater Data Centers		
1	Minimum Target Functional Duration for Terrestrial Data Centers (days)	0.6301
2	Maximum Target Functional Duration for Terrestrial Data Centers (days)	13.0471
3	Average Target Functional Duration for Terrestrial Data Centers (days)	6.7235
4	Minimum Target Functional Duration for Stratosphere Data Centers (days)	0.0012
5	Maximum Target Functional Duration for Stratosphere Data Centers (days)	11.596
6	Average Target Functional Duration for Stratosphere Data Centers (days)	6.926
7	Minimum Target Functional Duration for Underwater Data Centers(days)	0.2721
8	Maximum Target Functional Duration for Underwater Data Centers (days)	13.73
9	Average Target Functional Duration for Underwater Data Centers(days)	7.517
Scenario 1 – Mild Ballistic Nuclear Missile Attack		
10	Terrestrial Data Center Maximum Reduction in Functional Duration (%)	29.08
11	Terrestrial Data Center Minimum Reduction in Functional Duration (%)	0.19
12	Terrestrial Data Center Average Reduction in Functional Duration (%)	13.88
13	Stratosphere Data Center Maximum Reduction in Functional Duration (%)	29.69
14	Stratosphere Data Center Minimum Reduction in Functional Duration (%)	1.80
15	Stratosphere Data Center Average Reduction in Functional Duration (%)	13.88
16	Underwater Data Center Maximum Reduction in Functional Duration (%)	29.41
17	Underwater Data Center Minimum Reduction in Functional Duration (%)	0.28
18	Underwater Data Center Average Reduction in Functional Duration (%)	14.46
Scenario 2 – Moderate Ballistic Nuclear Missile Attack		
19	Terrestrial Data Center Maximum Reduction in Functional Duration (%)	58.97
20	Terrestrial Data Center Minimum Reduction in Functional Duration (%)	1.85
21	Terrestrial Data Center Average Reduction in Functional Duration (%)	25.16
22	Stratosphere Data Center Maximum Reduction in Functional Duration (%)	57.09
23	Stratosphere Data Center Minimum Reduction in Functional Duration (%)	2.99
24	Stratosphere Data Center Average Reduction in Functional Duration (%)	25.16
25	Underwater Data Center Maximum Reduction in Functional Duration (%)	59.62
26	Underwater Data Center Minimum Reduction in Functional Duration (%)	1.74
27	Underwater Data Center Average Reduction in Functional Duration (%)	31.71
Scenario 3 – Severe Ballistic Nuclear Missile Attack		
28	Terrestrial Data Center Maximum Reduction in Functional Duration (%)	83.69
29	Terrestrial Data Center Minimum Reduction in Functional Duration (%)	4.75
30	Terrestrial Data Center Average Reduction in Functional Duration (%)	40.06
31	Stratosphere Data Center Maximum Reduction in Functional Duration (%)	70.09
32	Stratosphere Data Center Minimum Reduction in Functional Duration (%)	0.73
33	Stratosphere Data Center Average Reduction in Functional Duration (%)	40.06
34	Underwater Data Center Maximum Reduction in Functional Duration (%)	79.78
35	Underwater Data Center Minimum Reduction in Functional Duration (%)	2.93
36	Underwater Data Center Average Reduction in Functional Duration (%)	49.93

vival-gateway in each of the region via optic fibre. This enables each underwater data center to have an active survival gateway given that the missile attack cannot occur in all regions concurrently. The flowchart for the diversity is in Fig. 9. In Fig. 9, the critical underwater network node has a database where the information on reachable survival gateways is stored.

5 Performance formulation

The performance metrics for the proposed network architecture is formulated in this section. The formulated metrics are: (1) Data center uptime (functional duration), and (2) Computing resource utilization. Let γ and ϑ denote the set of terrestrial data centers and stratosphere-based data

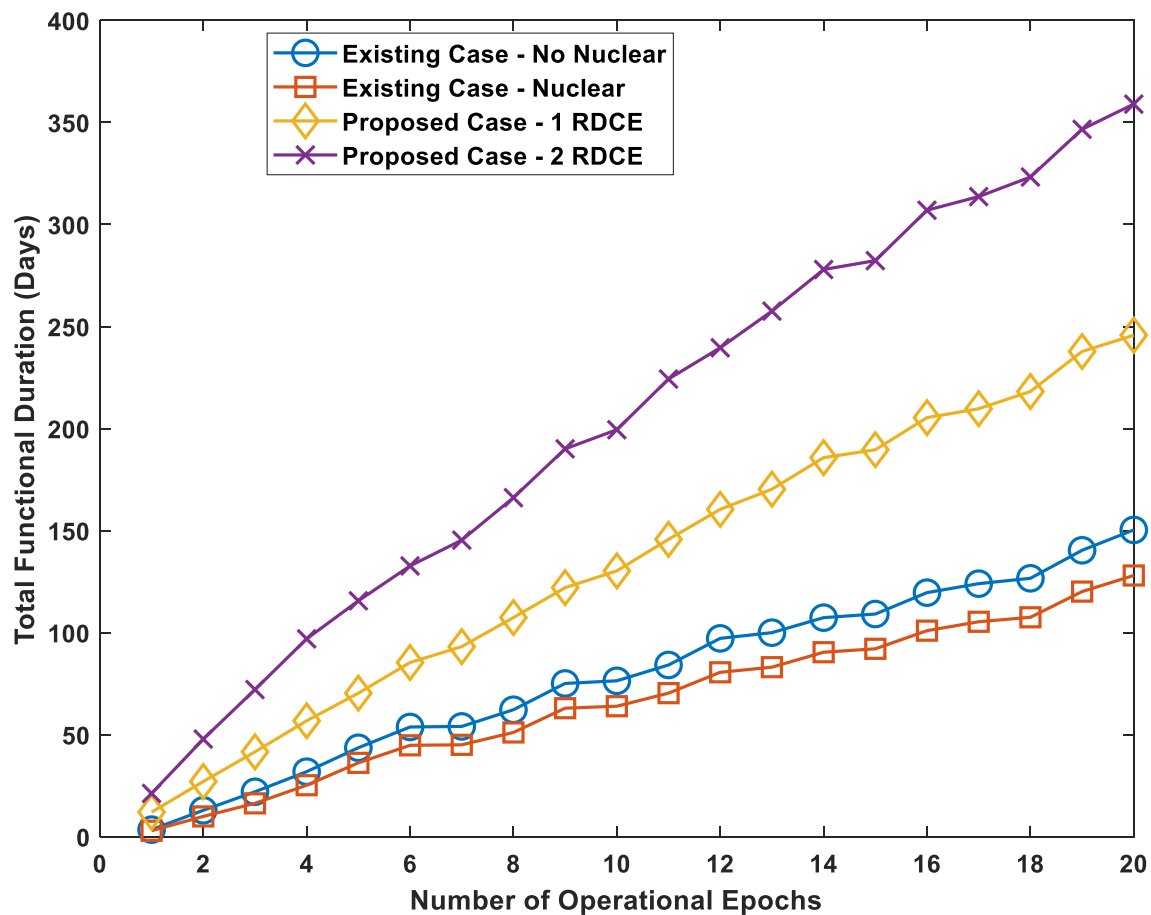


Fig. 10 Simulation results showing the results of the total functional duration (days) considering cases without and with the proposed mechanism in the case of a mild missile attack (Scenario 1) given different number of redundant data center entities (RDCEs)

centers. These data centers act as the redundant data center entities for deployed underwater data centers.

$$\gamma = \{\gamma_1, \gamma_2, \dots, \gamma_C\} \quad (10)$$

$$\vartheta = \{\vartheta_1, \vartheta_2, \dots, \vartheta_D\}. \quad (11)$$

In addition, let the reduction in the functional duration of the a^{th} underwater data center α_a observed for operation of up to epoch t_y be denoted $\psi_1(\alpha_a, t_y)$. The reduction is due to the occurrence of missile (nuclear) satisfies the condition $0 < \psi_1(\alpha_a, t_y) < 1$. The target functional duration for the i^{th} terrestrial data center is denoted $\theta(\gamma_c, t_y)$, $\gamma_c \in \gamma$. Furthermore, the target functional duration for the d^{th} stratosphere data center $\vartheta_d \in \vartheta$ is denoted $\theta(\vartheta_d, t_y)$. In this case, the target functional duration for redundant data center entities is dynamic and can be changed. This has been considered to incorporate the role of the distributed system in realizing redundant data centers. The functional duration before and after the incorporation of the proposed architecture is denoted as θ_1 and θ_2 , respectively.

$$\theta_1 = \sum_{y=1}^Y \sum_{a=1}^A (1 - \psi_1(\alpha_a, t_y)) \theta(\alpha_a, t_y) \quad (12)$$

$$\begin{aligned} \theta_2 = & \sum_{y=1}^Y \sum_{c=1}^C \sum_{d=1}^D \sum_{a=1}^A (1 - \psi_1(\alpha_a, t_y)) \theta(\alpha_a, t_y) \\ & + (1 - \psi_2(\gamma_c, t_y)) \theta(\gamma_c, t_y) \\ & + (1 - \psi_2(\vartheta_d, t_y)) \theta(\vartheta_d, t_y) \end{aligned} \quad (13)$$

$\psi_2(\gamma_c, t_y)$ And $\psi_2(\vartheta_d, t_y)$ are the proportion of time that γ_c and ϑ_d function as redundant models in the proposed solution at the y^{th} epoch t_y . The computing resource utilization is formulated for data center suitable for use as redundant data centers and with idle computing (storage) resources. In the absence of their use as redundant data center entities, these computing resources remain idle. Let $I(x, t_y) \in \{0, 1\}$, $x \in \{\gamma_c, \vartheta_d\}$ denote the redundant data center entity status of the entity x at the epoch t_y . The entity x does not function and functions as a redundant data center entity at epoch t_y when $I(x, t_y) = 0$ and $I(x, t_y) = 1$, respectively. The computing resource utilization before the use of the

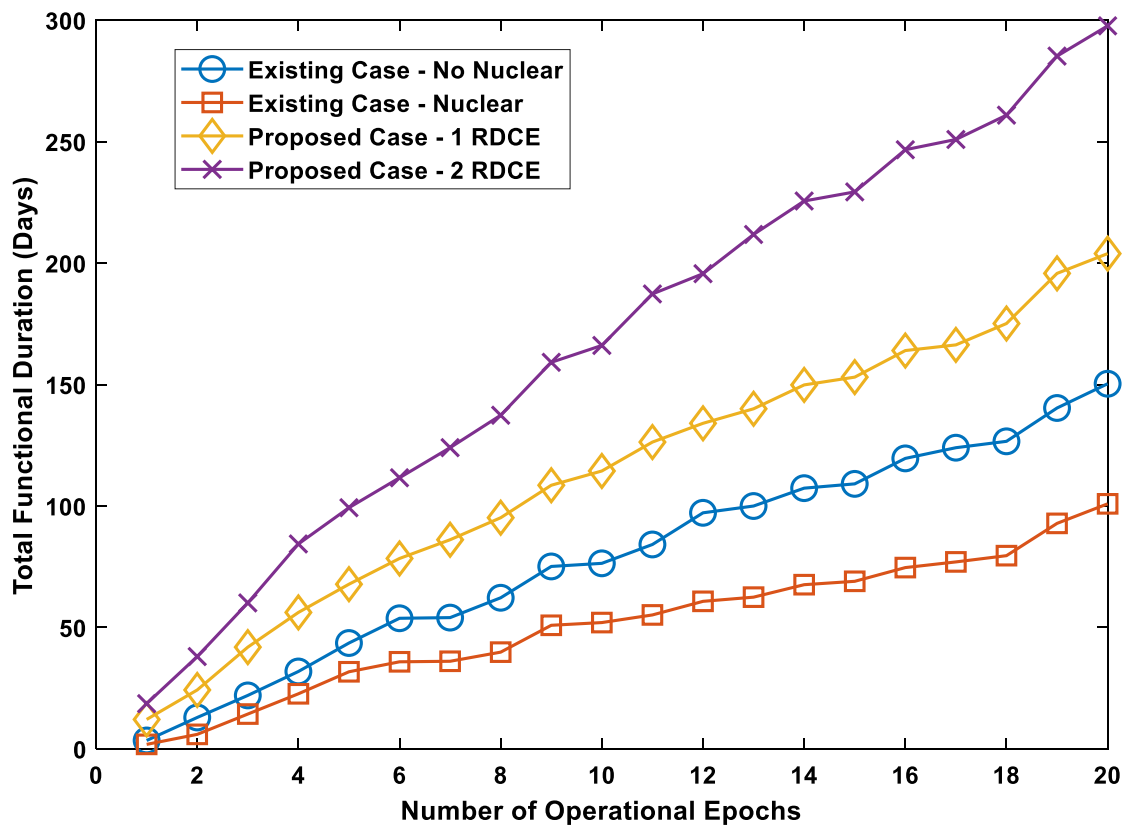


Fig. 11 Simulation results showing the results of the total functional duration (days) considering cases without and with the proposed mechanism in the case of a moderate missile attack (Scenario 2) given different number of redundant data center entities (RDCEs)

proposed network architecture is denoted as Γ_1 . The computing resource utilization after the use of the proposed network architecture is denoted as Γ_2 .

$$\Gamma_1 = \sum_{y=1}^Y \sum_{c=1}^C \sum_{d=1}^D \frac{|I(x = \gamma_c, t_y) = 0| C_1(x = \gamma_c, t_y)}{C_{\max}(x = \gamma_c)} + \frac{|I(x = \vartheta_d, t_y) = 0| C_1(x = \vartheta_d, t_y)}{C_{\max}(x = \vartheta_d)} \quad (14)$$

$$\Gamma_2 = \sum_{y=1}^Y \sum_{c=1}^C \sum_{d=1}^D \frac{(|I(x = \gamma_c, t_y) = 0| + |I(x = \gamma_c, t_y) = 1|) C_1(x = \gamma_c, t_y)}{C_{\max}(x = \gamma_c)} + \frac{(|I(x = \vartheta_d, t_y) = 0| + |I(x = \vartheta_d, t_y) = 1|) C_1(x = \vartheta_d, t_y)}{C_{\max}(x = \vartheta_d)} \quad (15)$$

$C_1(x, t_y)$ and $C_{\max}(x)$ are the amount of idle computing resources aboard x at the epoch t_y and the maximum computing resources aboard the entity x , respectively.

Furthermore, the number of packets forwarding paths is an important metric that is also formulated. The number of packets forwarding paths is an important parameter that should be enhanced by the proposed diversity approach. In deriving the number of packets forwarding paths, the data center is deemed to have a networking and communication system that comprises routers. The routers utilize

intelligent mechanisms and form packet forwarding routes and paths. This is done in a manner influenced by the functioning of onboard intelligent routing algorithms. The modelling of the number of packets forwarding paths has not been considered as routers host different intelligent algorithms and logic.

Let η denote the set of routers such that:

$$\eta = \{\eta_{UDC}, \eta_{RDCE}\} \quad (16)$$

η_{UDC} and η_{RDCE} are the set of network path determining routers aboard the underwater data center and redundant data center entity, respectively.

$$\eta_{UDC} = \{\eta_{UDC}^1, \eta_{UDC}^2, \dots, \eta_{UDC}^V\} \quad (17)$$

$$\eta_{RDCE} = \{\eta_{RDCE}^1, \eta_{RDCE}^2, \dots, \eta_{RDCE}^D\} \quad (18)$$

Each router in η_{UDC} and η_{RDCE} has a path formation factor. The path formation factor for routers $\eta_{UDC}^v, \eta_{UDC}^v \in \eta_{UDC}$ and $\eta_{RDCE}^d, \eta_{RDCE}^d \in \eta_{RDCE}$ at the epoch t_y are $\zeta_1(\eta_{UDC}^v, t_y)$, and $\zeta_1(\eta_{RDCE}^d, t_y)$, respectively. Each router arising from the path formation factor has an associated route nuclear resiliency. The router nuclear resiliency describes the ability of a route to support packet transmission after a nuclear attack. The route nuclear

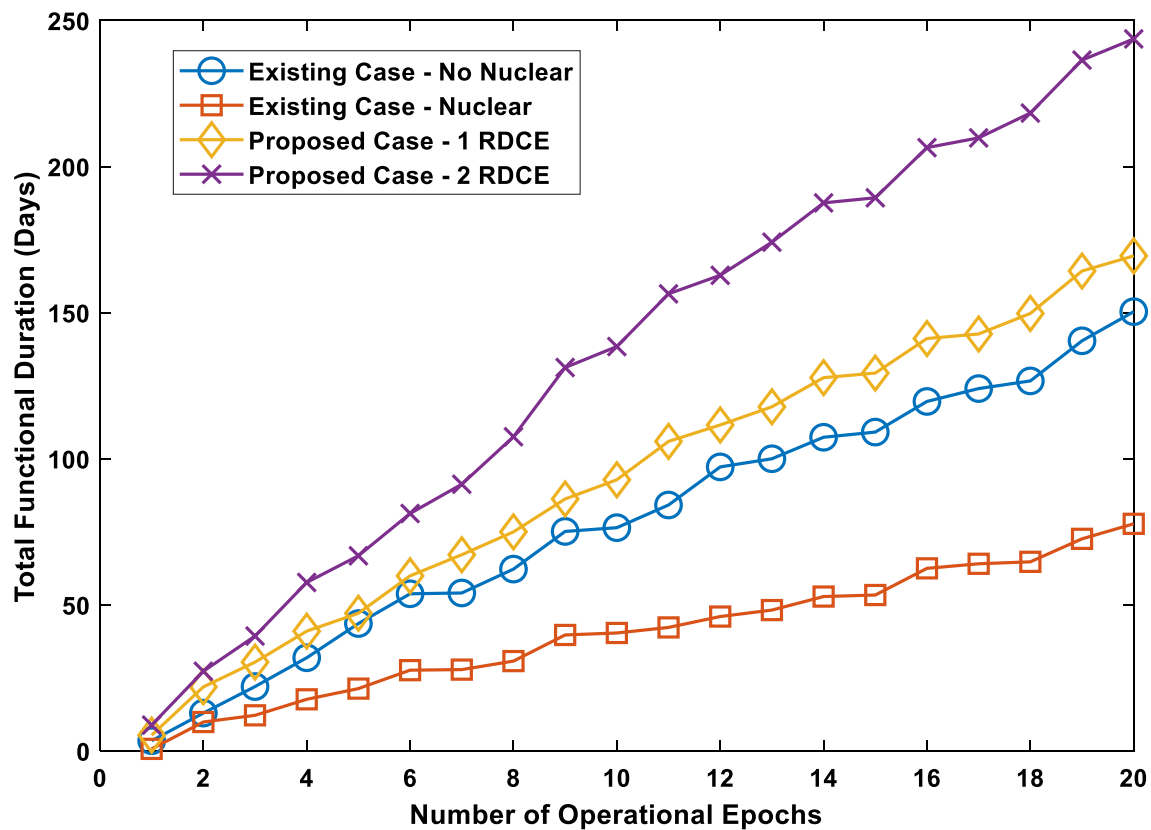


Fig. 12 Simulation results showing the results of the total functional duration (days) considering cases without and with the proposed mechanism in the case of a severe missile attack (Scenario 3) given different number of redundant data center entities (RDCEs)

resiliency is route dependent and the set of routes associated with the router entities η_{UDC}^v and η_{RDCE}^d are given as:

$$\eta_{UDC}^v = \{\eta_{UDC}^{v,1}, \eta_{UDC}^{v,2}, \dots, \eta_{UDC}^{v,Q}\} \quad (19)$$

$$\eta_{RDCE}^d = \{\eta_{RDCE}^{d,1}, \eta_{RDCE}^{d,2}, \dots, \eta_{RDCE}^{d,F}\} \quad (20)$$

The route resiliency factor for the routes $\eta_{UDC}^{v,q}, \eta_{UDC}^{v,q} \in \eta_{UDC}^v$ and $\eta_{RDCE}^{d,f}, \eta_{RDCE}^{d,f} \in \eta_{RDCE}^d$ at the epoch t_y are denoted $\zeta_2(\eta_{UDC}^{v,q}, t_y)$, and $\zeta_2(\eta_{RDCE}^{d,f}, t_y)$, respectively. A high route resiliency factor implies that a given route is associated with a higher number of branching routes. In addition, a low route resiliency factor implies that a given route has a low number of branching routes. The route resiliency factor is the number of redundant routes associated with a route involved in packet transmission.

The number of packets forwarding paths in the existing case given the occurrence of a nuclear attack is denoted A_1 and given as:

$$A_1 = \sum_{y=1}^Y \sum_{v=1}^V \sum_{q=1}^Q (\zeta_1(\eta_{UDC}^v, t_y) \zeta_2(\eta_{UDC}^{v,q}, t_y)) (1 - B_1(\eta_{UDC}^v, t_y)) \quad (21)$$

$B_1(\eta_{UDC}^v, t_y)$ is the nuclear route extinction factor. It describes the impact of a nuclear attack on the links associated with the router η_{UDC}^v at the epoch t_y . In a comparable manner, the redundant data center entity related nuclear route extinction factor is denoted as $B_1(\eta_{RDCE}^d, t_y)$.

The number of packets forwarding paths after the incorporation of the proposed architecture given the occurrence of a nuclear attack on the inter-datacenter network is denoted A_2 and given as:

$$A_2 = \sum_{y=1}^Y \left(\sum_{v=1}^V \sum_{q=1}^Q (\zeta_1(\eta_{UDC}^v, t_y) \zeta_2(\eta_{UDC}^{v,q}, t_y)) \right. \\ \left. (1 - B_1(\eta_{UDC}^v, t_y)) + \sum_{d=1}^D \sum_{f=1}^F \right. \\ \left. (\zeta_1(\eta_{RDCE}^d, t_y) \zeta_2(\eta_{RDCE}^{d,f}, t_y)) (1 - B_1(\eta_{RDCE}^d, t_y)) \right) \quad (22)$$

The relations in (21) and (22) describe the number of packets forwarding links associated with routers and other packet forwarding entities. The formulation in (22) recognizes the incorporation of the redundant data center entity. This enhances the resiliency of the inter-datacenter

Table 3 Simulation parameters for the considered scenarios (with the effect of the mushroom clouds)

S/N	Parameter	Value
Target Functional Duration for Terrestrial, Stratosphere, and Underwater Data Centers		
1	Minimum Target Functional Duration for Terrestrial Data Centers (days)	0.4739
2	Maximum Target Functional Duration for Terrestrial Data Centers (days)	13.6564
3	Average Target Functional Duration for Terrestrial Data Centers (days)	7.1178
4	Minimum Target Functional Duration for Stratosphere Data Centers (days)	0.4857
5	Maximum Target Functional Duration for Stratosphere Data Centers (days)	13.8395
6	Average Target Functional Duration for Stratosphere Data Centers (days)	8.707
7	Minimum Target Functional Duration for Underwater Data Centers(days)	0.3801
8	Maximum Target Functional Duration for Underwater Data Centers(days)	13.22
9	Average Target Functional Duration for Underwater Data Centers(days)	7.5496
Scenario 1 – Mild Ballistic Nuclear Missile Attack		
10	Terrestrial Data Center Maximum Reduction in Functional Duration (%)	29.08
11	Terrestrial Data Centre Minimum Reduction in Functional Duration (%)	0.19
12	Terrestrial Data Center Average Reduction in Functional Duration (%)	13.88
13	Stratosphere Data Center Maximum Reduction in Functional Duration (%)	29.69
14	Stratosphere Data Center Minimum Reduction in Functional Duration (%)	1.80
15	Stratosphere Data Center Average Reduction in Functional Duration (%)	13.88
16	Underwater Data Center Maximum Reduction in Functional Duration (%)	29.83
17	Underwater Data Center Minimum Reduction in Functional Duration (%)	1.62
18	Underwater Data Center Average Reduction in Functional Duration (%)	15.09
Scenario 2 – Moderate Ballistic Nuclear Missile Attack		
19	TDC Maximum Reduction in Functional Duration (%)	50.06
20	TDC Minimum Reduction in Functional Duration (%)	2.75
21	TDC Average Reduction in Functional Duration (%)	23.26
22	SDC Maximum Reduction in Functional Duration (%)	63.04
23	SDC Minimum Reduction in Functional Duration (%)	0.33
24	SDC Average Reduction in Functional Duration (%)	23.26
25	Underwater Data Center Maximum Reduction in Functional Duration (%)	53.82
26	Underwater Data Center Minimum Reduction in Functional Duration (%)	3.25
27	Underwater Data Center Average Reduction in Functional Duration (%)	28.98
Scenario 3 – Severe Ballistic Nuclear Missile Attack		
28	Terrestrial Data Center Maximum Reduction in Functional Duration (%)	81.19
29	Terrestrial Data Center Minimum Reduction in Functional Duration (%)	3.64
30	Terrestrial Data Center Average Reduction in Functional Duration (%)	38.97
31	Stratosphere Data Center Maximum Reduction in Functional Duration (%)	41.13
32	Stratosphere Data Center Minimum Reduction in Functional Duration (%)	4.16
33	Stratosphere Data Center Average Reduction in Functional Duration (%)	38.97
34	Underwater Data Center Maximum Reduction in Functional Duration (%)	73.06
35	Underwater Data Center Minimum Reduction in Functional Duration (%)	9.51
36	Underwater Data Center Average Reduction in Functional Duration (%)	48.93

network. However, the formulation in (22) has not considered the proposed diversity approach. The redundancy component associated with $\zeta_1(\eta_{UDC}^v, t_y)$, $\zeta_2(\eta_{UDC}^{v,q}, t_y)$ and

$B_1(\eta_{UDC}^v, t_y)$ are $\zeta_1 t(\eta_{UDC}^v, t_y)$, $\zeta_2 t(\eta_{UDC}^{v,q}, t_y)$ and $B_1 t(\eta_{UDC}^v, t_y)$, respectively.

The number of packets forwarding paths considering the proposed diversity approach A_3 is given as:

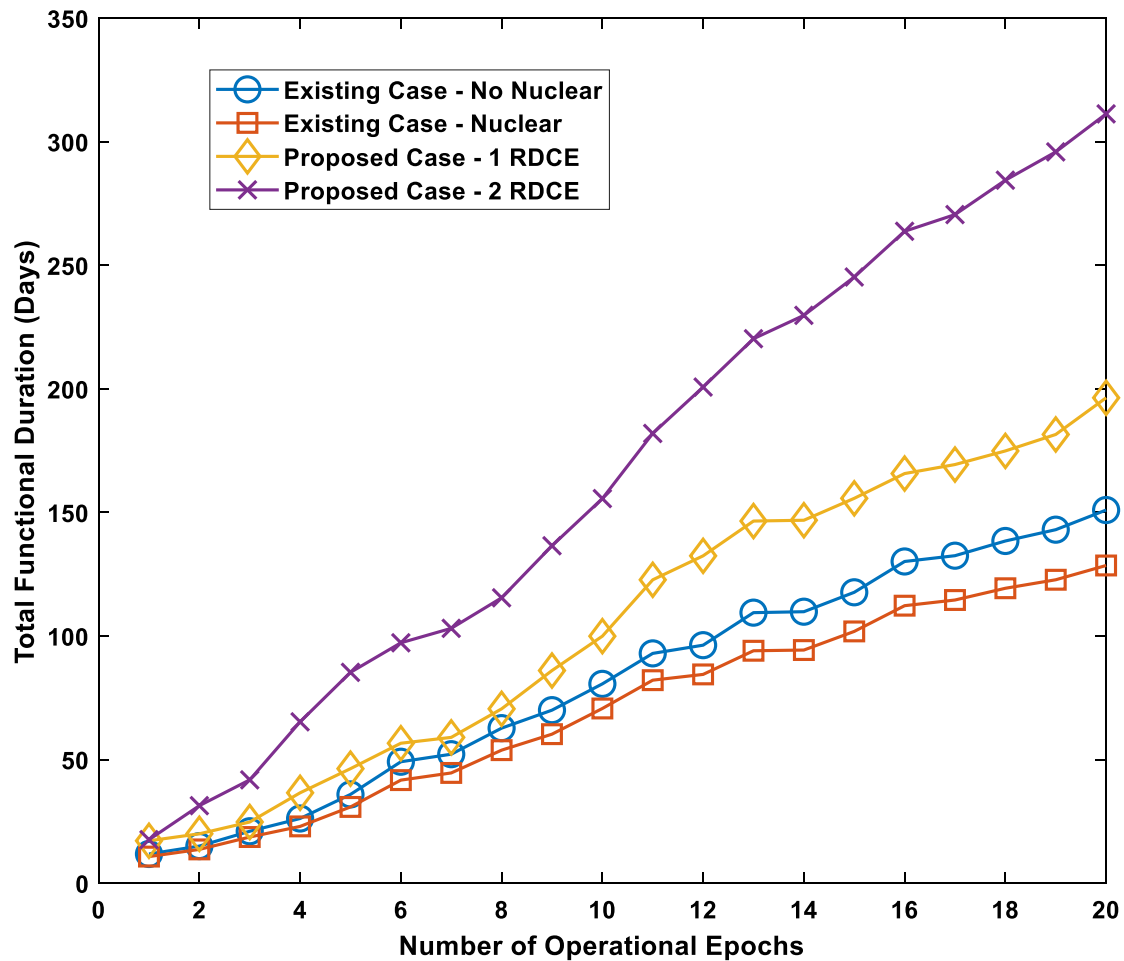


Fig. 13 Simulation results showing the results of the total functional duration (days) considering cases without and with the proposed mechanism in the case of a mild missile attack (Scenario 1

considering the effect of a mushroom cloud) given different number of redundant data center entities (RDCEs)

$$\begin{aligned}
 A_3 = & \sum_{y=1}^Y \left(\sum_{v=1}^V \sum_{q=1}^Q ((\zeta_1(\eta_{UDC}^v, t_y) \zeta_2(\eta_{UDC}^{v,q}, t_y)) \right. \\
 & (1 - B_1(\eta_{UDC}^v, t_y)) + (\zeta_1'(\eta_{UDC}^v, t_y) \zeta_2'(\eta_{UDC}^{v,q}, t_y)) \\
 & (1 - B_1'(\eta_{UDC}^v, t_y))) + \sum_{d=1}^D \sum_{f=1}^F \\
 & \left(\zeta_1(\eta_{RDCE}^d, t_y) \zeta_2(\eta_{RDCE}^{d,f}, t_y) \right) \\
 & (1 - B_1(\eta_{RDCE}^d, t_y)) + (\zeta_1'(\eta_{UDC}^v, t_y) \zeta_2'(\eta_{UDC}^{v,q}, t_y)) \\
 & (1 - B_1'(\eta_{UDC}^v, t_y)))
 \end{aligned} \quad (23)$$

6 Performance evaluation

The performance benefits and analysis of the proposed mechanism is presented in this section. The metrics are: (1) Functional duration, (2) Computing resource utilization, and (3) Number of packets forwarding paths.

These metrics describe the survivability of the proposed network architecture. The functional duration i.e., the operational uptime is enhanced when the network architecture is utilized. This is because the occurrence of missile attack from the submarine does not lead to the occurrence

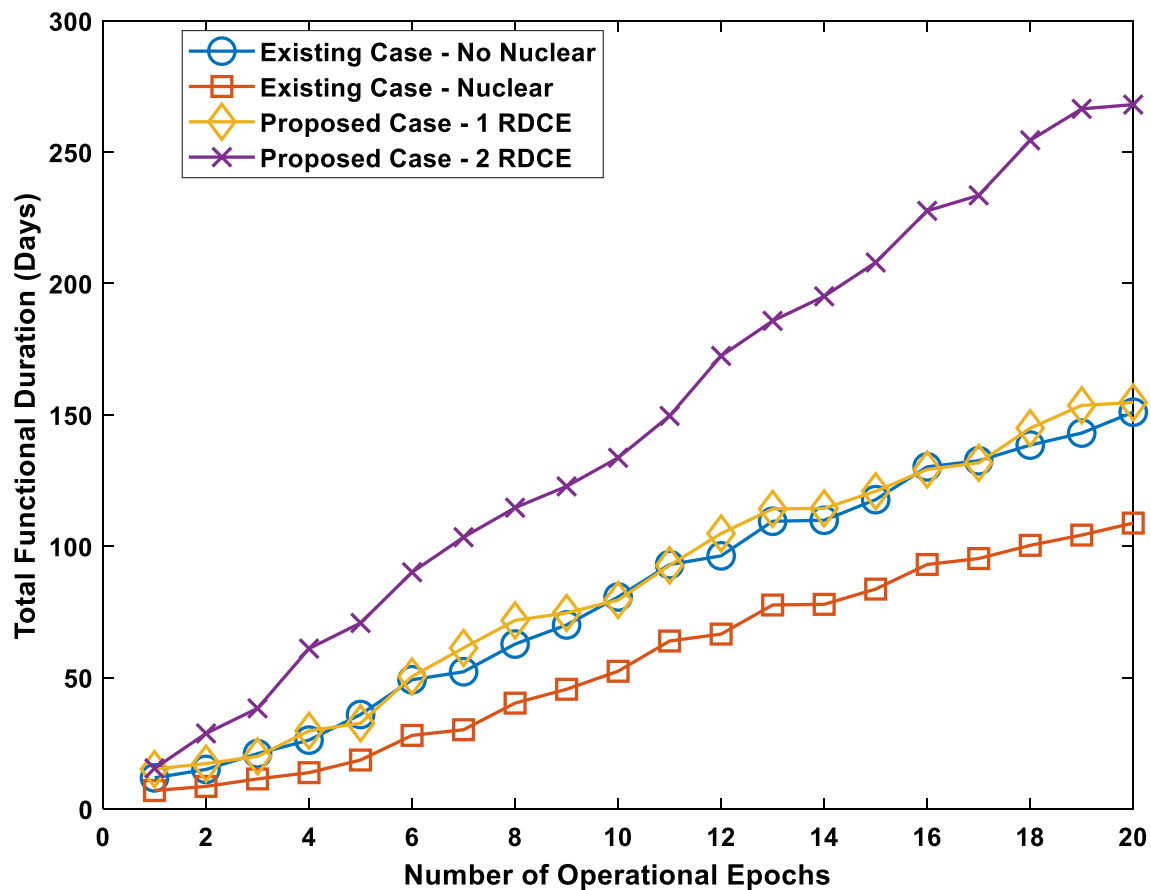


Fig. 14 Results showing the total functional duration considering cases without and with the proposed mechanism in a moderate missile attack (Scenario 2 considering the mushroom cloud) given different number of redundant data center entities (RDCEs)

of downtime. In this case, the performance evaluation is done using the relations in (12) and (13). The inclusion of redundant data center entities reduces the incidence of idling computing resources. This results in an improvement in the computing resource utilization. The performance evaluation is done using the formulated relations presented in (14) and (15).

The conduct of the performance evaluation is done via MATLAB performance simulation. The use of performance emulation tools has not been used. This is because of a paucity of emulation tools for communication networks with capability to observe the behaviour of underwater data centers. The use of underwater data centers is still at a nascent stage. However, the simulation of the formulated mathematical models in this case is feasible and applicable.

In adopting the performance evaluation procedure, existing research such as that in Guo et al. Aug. (2009) which focuses on modular data centers is recognized. The modular data center in Guo et al. Aug. (2009) is realized by placing servers in shipping containers. They are placed in the terrestrial environment and not in the underwater

environment. The operational environment of the BCube modular data center in Guo et al. Aug. (2009) is the terrestrial environment. The terrestrial environment differs from the submarine environment hosting the underwater data center. In addition, discussion in Alqahtani et al. (2018), Lin et al. (2012) shows that the challenge is realizing low latency routing. The low latency routing is realized for low-cost terrestrial data centers. This is different from the consideration focusing on underwater data centers in the underwater environment. In this case, the underwater data center has a high susceptibility to functionality loss from submarine launched missiles.

The discussion in this section is divided into three aspects. The first aspect focuses on the metric of the operational duration. The second aspect presents and discusses the simulation and performance results associated with the computing resource utilization. The computing resource utilization is associated with the functionality of redundant data center entity. It is associated with the proposed network architecture. The third evaluates the results for number of packets forwarding path metric in proposed network architecture.

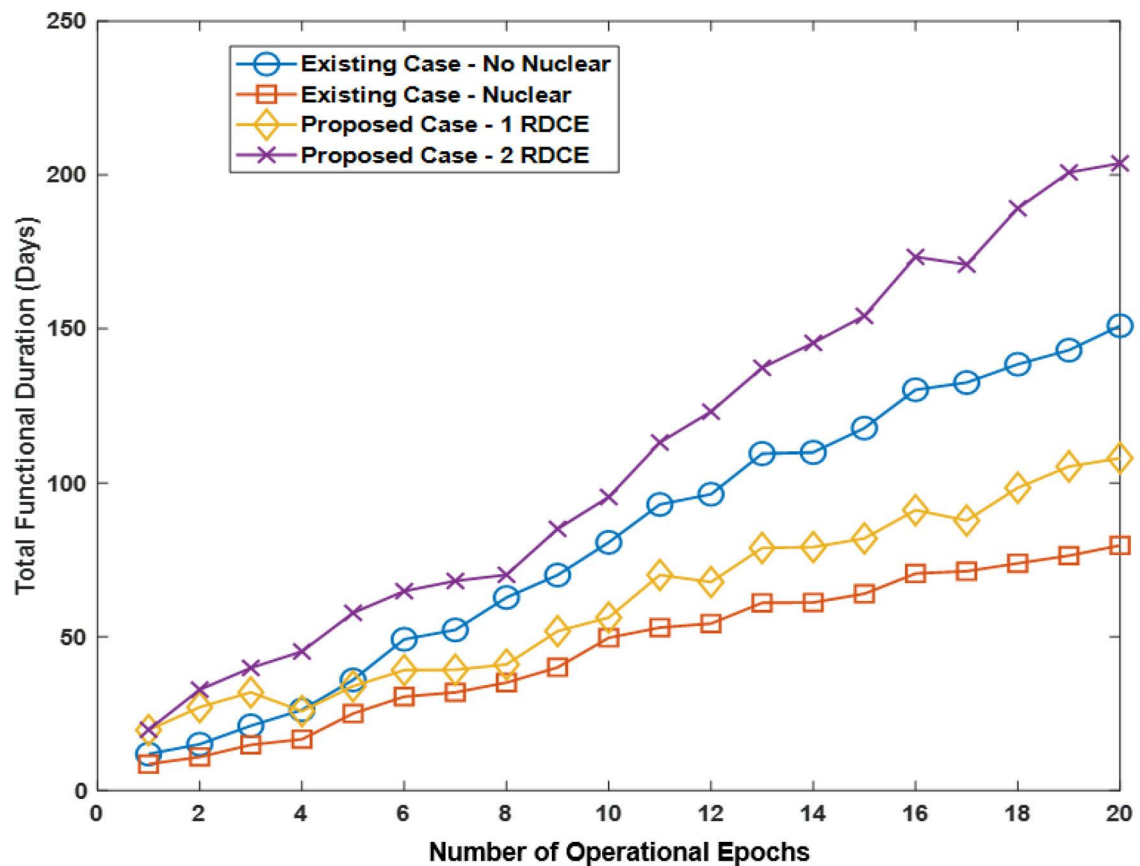


Fig. 15 Results showing the total functional duration without and with the proposed mechanism in a severe missile attack (Scenario 3 considering the mushroom cloud) given different number of redundant data center entities (RDCEs)

A. Performance Evaluation: Operational Duration

The simulation parameters are in Table 2. The simulation scenario and context being considered comprises underwater, terrestrial, and stratosphere data centers. Each of the underwater, terrestrial or stratosphere data center has servers that execute data storage, processing, and algorithm execution. In addition, each of the underwater, terrestrial or stratosphere data center has own designated functional duration. They also have a given proportion of time for which they function as an redundant data center entity. The performance simulation parameters are presented in Table 2.

In Table 2, the simulation parameter has been selected for a two-week (14 days) operational duration. In this case, the maximum operational duration has values that span between 1 and 14 days. Each of the redundant data center candidate entities functions for a proportion of time. During this time duration, a given proportion of their resources enable redundant data center entity functionality. The data centers that can function as redundant data center entities are terrestrial, underwater or stratosphere data center. This proportion in percentage can be significantly high for underutilized redundant data center entity. In addition, the

proportion in percentage is low for maximally utilized servers aboard the data center entity.

The simulation values used in this regard considers the computing resources aboard the underwater, terrestrial or stratosphere data center for a select number of servers. These simulation parameters have been selected to be variable. In addition, the terrestrial data center and stratosphere data center are the dominantly active redundant data center entities and not underwater data centers. The rationale for this is the prevention of the conduct a greedy estimate procedure during the simulation. The considered simulation scenario comprises underwater, terrestrial and stratosphere data centers. Each of the underwater data center, terrestrial data center or stratosphere data center has servers that execute data storage and algorithm execution. In addition, each of the underwater, terrestrial or stratosphere data center has own functional duration. During this functional duration, each of either of the underwater data center, terrestrial data center or stratosphere data center acts as an redundant data center entity. In Table 2, the maximum operational duration has value that span between 1 and 14 days. The computing resources aboard the underwater, terrestrial or stratosphere data center have been

Table 4 Parameters for Investigating Computing Resource Utilization

S/N	Parameter	Value
1	Underwater Data Center Maximum Amount of Computing Resources	4024.1 GBytes
2	Underwater Data Center Average Amount of Computing Resources	2299.5 GBytes
3	Underwater Data Center Minimum Amount of Computing Resources	312.15 GBytes
4	Stratosphere Data Center Maximum Amount of Computing Resources	3022.5 GBytes
5	Stratosphere Data Center Average Amount of Computing Resources	1201.6 GBytes
6	Stratosphere Data Center Minimum Amount of Computing Resources	249.44 GBytes
7	Terrestrial Data Center Maximum Amount of Computing Resources	5140.9 GBytes
8	Terrestrial Data Center Average Amount of Computing Resources	3082.5 GBytes
9	Terrestrial Data Center Minimum Amount of Computing Resources	23.84 GBytes
Simulation Parameters Associated with First Epoch of Simulation		
1	Underwater Data Center Maximum Proportion of Time as Redundant Data Center Entity (%)	97.01
2	Underwater Data Center Average Proportion of Time as Redundant Data Center Entity (%)	54.59
3	Underwater Data Center Minimum Proportion of Time as Redundant Data Center Entity (%)	3.69
4	Stratosphere Data Center Maximum Proportion of Time as Redundant Data Center Entity (%)	99.98
5	Stratosphere Data Center Average Proportion of Time as Redundant Data Center Entity (%)	59.91
6	Stratosphere Data Center Minimum Proportion of Time as Redundant Data Center Entity (%)	3.69
7	Terrestrial Data Center Maximum Proportion of Time as Redundant Data Center Entity (%)	98.75
8	Terrestrial Data Center Average Proportion of Time as Redundant Data Center Entity (%)	56.38
9	Terrestrial Data Center Minimum Proportion of Time as Redundant Data Center Entity (%)	1.37
Simulation Parameters Associated with Second Epoch of Simulation		
10	Underwater Data Center Maximum Proportion of Time as Redundant Data Center Entity (%)	99.26
11	Underwater Data Center Average Proportion of Time as Redundant Data Center Entity (%)	57.00
12	Underwater Data Center Minimum Proportion of Time as Redundant Data Center Entity (%)	5.22
13	Stratosphere Data Center Maximum Proportion of Time as Redundant Data Center Entity (%)	82.91
14	Stratosphere Data Center Average Proportion of Time as Redundant Data Center Entity (%)	47.14
15	Stratosphere Data Center Minimum Proportion of Time as Redundant Data Center Entity (%)	5.22
16	Terrestrial Data Center Maximum Proportion of Time as Redundant Data Center Entity (%)	66.7
17	Terrestrial Data Center Average Proportion of Time as Redundant Data Center Entity (%)	31.3
18	Terrestrial Data Center Minimum Proportion of Time as Redundant Data Center Entity (%)	0.09

considered for a select number of servers. The simulation parameters have been selected to be variable thereby enabling the conduct of stochastic simulation. In addition, the terrestrial and stratosphere data center are the dominant redundant data center entities. The rationale for this is the prevention of the conduct of a greedy estimate procedure during the simulation.

In addition, the simulation is done for three scenarios. These scenarios consider different scales of a nuclear attack. This is because submarine launched ballistic missiles has varying effects on underwater, terrestrial and stratosphere data centers in the proposed redundancy pair-oriented mechanism and network architecture. The first scenario, second scenario and third scenario consider mild ballistic nuclear missile attack, moderate ballistic missile attack and severe ballistic missile attack, respectively. The results for functional duration (days) are obtained for the

case of mild ballistic, moderate ballistic and severe ballistic nuclear missile attacks. The functional duration for the case of mild ballistic, moderate ballistic and severe ballistic nuclear missile attacks are in Figs. 9, 10, and 11, respectively. In the simulation, the occurrence of a missile attack in the considered scenarios results in a varying reduction in the functional duration. The reduction is associated with either the underwater data center, terrestrial data center or stratosphere data center.

Analysis of the results in Figs. 10, 11, and 12, shows that the total functional duration reduces with the increasing severity of a ballistic missile nuclear attack. This is because an increasing severity is associated with an increasing degradation in the expected functional duration.

In Scenario 1, the use of the proposed redundant data center entity in the networking architecture is observed to enhance the total functional duration. The use of 1

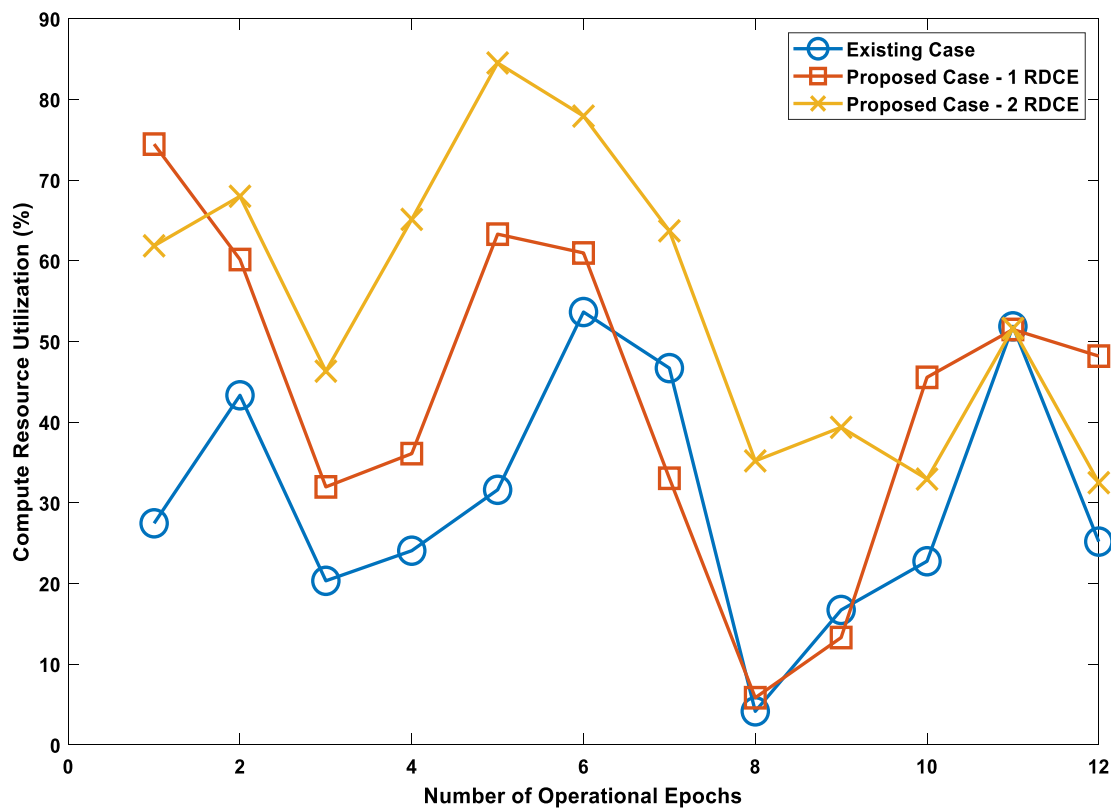


Fig. 16 Simulation Results for the Compute Resource Utilization in the First Epoch in the network scenario considering the evaluation of the performance of the proposed network architecture having a variable number of redundant data center entities

redundant data center entity in comparison to the case when a nuclear attack occurs enhances the total functional duration by an average of 52.9%. The use of 2 redundant data center entities in comparison to the case when a nuclear attack occurs enhances the total functional duration by an average of 69.6%. An increase in the number of redundant data center entities by 50% from 1 to 2 enhances the total functional duration by 35.8% on average. Furthermore, the non-use of the redundant data center entity in the existing case results in functional duration reduction. An occurrence of a nuclear attack as observed in Scenario 1 results in a degradation of the total functional duration by 17.1% on average.

Furthermore, the use of the proposed redundant data center entity in the proposed networking architecture enhances the total functional duration in Scenario 2. In scenario 2, the use of 1 redundant data center entity enhances the total functional duration by an average of 57.9%. Furthermore, the use of 2 redundant data center entities in comparison to the case when a nuclear attack occurs enhance the total functional duration. In this case, the total functional duration is enhanced by an average of 71.5%. In addition, increasing the number of redundant data center entities by 50% from 1 to 2 enhances the functional duration by 32.4% on average. Furthermore, the

non-use of the redundant data center entity in the existing case given an occurrence of a nuclear attack results in a reduced total functional duration. The total functional duration as observed in Scenario 1 reduces by 36% on average.

In addition, the use of the redundant data center entity in the proposed networking architecture enhances the total functional duration in Scenario 3 (case of Severe Missile Attack). The use of 1 redundant data center entity enhances the total functional duration by an average of 58.4%. In addition, the use of 2 redundant data center entities in comparison to the case when a nuclear attack occurs enhance the functional duration. The total functional duration is enhanced by an average of 70.9%. In addition, an increase in the number of redundant data center entities by 50% from 1 to 2 enhance the total functional duration by 30.3% on average. The non-use of the redundant data center entity in the existing case given an occurrence of a nuclear attack as observed in Scenario 1 results in degradation of the total functional duration by 49.2% on average.

The simulation procedure also considers the case where the occurrence of a missile attack in each of the scenarios is associated with the occurrence of a mushroom cloud. The occurrence of a mushroom cloud is often linked to a nuclear missile effect as seen in Won and Lee (2020). This

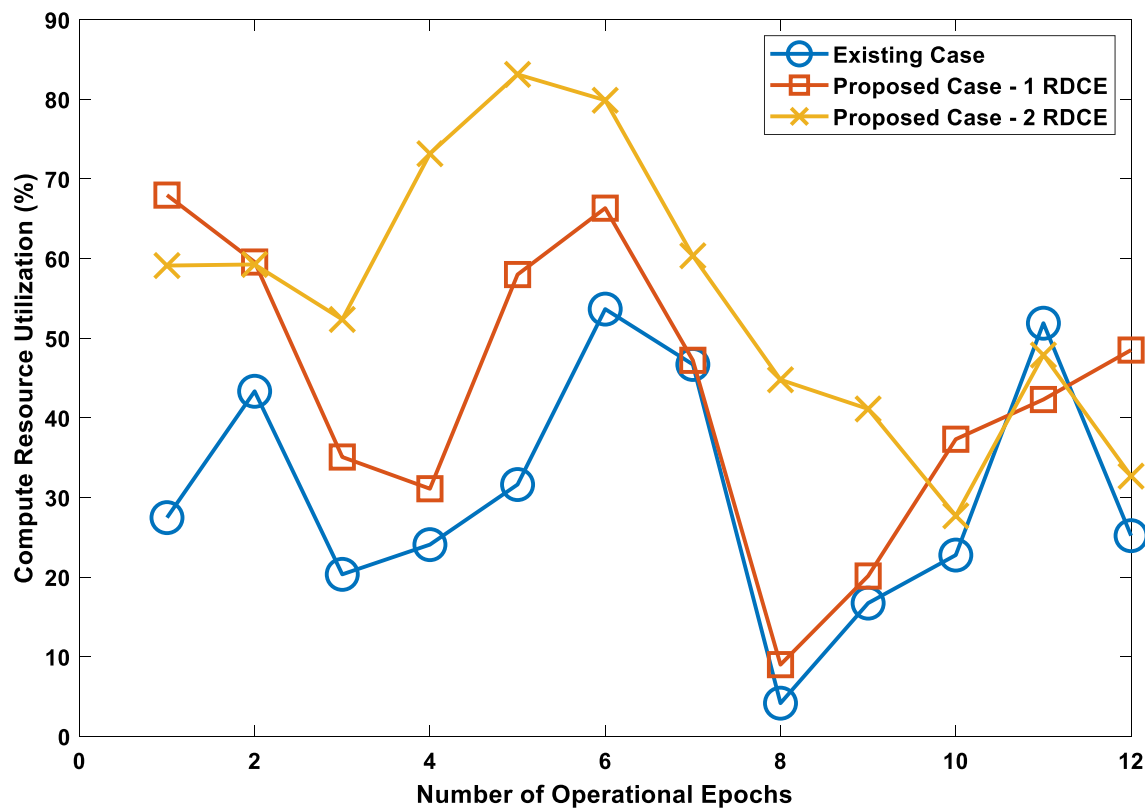


Fig. 17 Simulation Results for the Compute Resource Utilization in the Second Epoch in the network scenario considering the evaluation of the performance of the proposed network architecture having a variable number of redundant data center entities

leads to the release of particles into the atmosphere. These particles cause the attenuation of radio waves enabling wireless communications between stratosphere data centers. In this case, the mushroom cloud has a significant altitude. This is feasible as seen in missile with high altitude mushroom clouds (Congressional Research Office 2022). In this case, the simulation parameters are presented in Table 3. The results in Scenario 1, Scenario 2 and Scenario 3 are in Fig. 13, Fig. 14, and Fig. 15, respectively.

For the case where the effect of a mushroom cloud is incorporated, the results in Figs. 12, 13 and 14 show that there is a reduction in the total functional duration. This is in comparison with the results in Figs. 10, 11 and 12. In Scenario 1, the use of 1 redundant data center entity is enhance the total functional duration by an average of 31.8%. Furthermore, the use of 2 redundant data center entities in comparison to the case when a nuclear attack occurs is enhance the total functional duration by an average of 56.7%.

In addition, an increase in the number of redundant data center entities by 50% from 1 to 2 is observed to enhance the total functional duration by 36.3% on average. The non-use of the redundant data center entity in the existing case given a nuclear attack as observed in Scenario 1

reduces the total functional duration by 17.1% on average. In the case of Scenario 2, the use of the proposed scenario in a case comprising 1 redundant data center entity enhances the total functional duration by an average of 38.3%. Furthermore, the use of 2 redundant data center entities enhances the total functional duration by an average of 63.5%. An increase in the number of redundant data center entities by 50% from 1 to 2 enhances the duration by 40.5% on average. In Scenario 3, the use of 1 redundant data center entity and 2 redundant data center entities enhances the total functional duration by an average of 27.7% and 57.3%, respectively. An increase in the number of redundant data center entities by 50% from 1 to 2 improves the total functional duration by 39.1% on average.

B. Performance Evaluation: Computing Resource Utilization (Redundant Data Center Entity Functionality)

The discussion here presents the performance evaluation results associated with the computing resource utilization in the proposed network architecture. The computing resource utilization describes the capability of the relating multi-contextual networked computing entities to store and execute data processing. This is important due to the increasing role of data in future network and subscriber

Table 5 Performance Simulation Parameters used in investigating improvement in number of paths

S/N	Parameter	Value
1	Number of Routers in Underwater Data Center and Redundant Data Center Entity	12
2	Number of Routes associated with Underwater Data Center and Redundant Data Center Entity	288
3	Minimum Path Formation Factor of Underwater Data Center	16.8%
4	Mean Path Formation Factor of Underwater Data Center	52.2%
5	Maximum Path Formation Factor of Underwater Data Center	87.4%
6	Minimum Path Formation Factor of Redundant Data Center Entity	7.8%
7	Mean Path Formation Factor of Redundant Data Center Entity	39.1%
8	Maximum Path Formation Factor of Redundant Data Center Entity	86%
9	Minimum Route Resiliency Factor of Underwater Data Center	0.5%
10	Mean Route Resiliency Factor of Underwater Data Center	46.7%
11	Maximum Route Resiliency Factor of Underwater Data Center	99%
12	Minimum Route Resiliency Factor of Redundant Data Center Entity	0.1%
13	Mean Route Resiliency Factor of Redundant Data Center Entity	48.4%
14	Maximum Route Resiliency Factor of Redundant Data Center Entity	99%
15	Minimum Nuclear Route Extinction Factor of Underwater Data Center	0.1%
16	Mean Nuclear Route Extinction Factor of Underwater Data Center	50.6%
17	Maximum Nuclear Route Extinction Factor of Underwater Data Center	99%
18	Minimum Nuclear Route Extinction Factor of Redundant Data Center Entity	0.71%
19	Mean Nuclear Route Extinction Factor of Redundant Data Center Entity	53.9%
20	Maximum Nuclear Route Extinction Factor of Redundant Data Center Entity	99%
Diversity Incorporation in the Proposed Network Architecture		
21	Minimum Path Formation Factor of Underwater Data Center	17%
22	Mean Path Formation Factor of Underwater Data Center	62.8%
23	Maximum Path Formation Factor of Underwater Data Center	98%
24	Minimum Path Formation Factor of Redundant Data Center Entity	15.8%
25	Mean Path Formation Factor of Redundant Data Center Entity	50.6%
26	Maximum Path Formation Factor of Redundant Data Center Entity	97%
27	Minimum Route Resiliency Factor of Underwater Data Center	0.02%
28	Mean Route Resiliency Factor of Underwater Data Center	47.5%
29	Maximum Route Resiliency Factor of Underwater Data Center	99%
30	Minimum Route Resiliency Factor of Redundant Data Center Entity	0.3%
31	Mean Route Resiliency Factor of Redundant Data Center Entity	49.2%
32	Maximum Route Resiliency Factor of Redundant Data Center Entity	99%
33	Minimum Nuclear Route Extinction Factor of Underwater Data Center	0.06%
34	Mean Nuclear Route Extinction Factor of Underwater Data Center	49%
35	Maximum Nuclear Route Extinction Factor of Underwater Data Center	99%
36	Minimum Nuclear Route Extinction Factor of Redundant Data Center Entity	0.01%
37	Mean Nuclear Route Extinction Factor of Redundant Data Center Entity	51.1%
38	Maximum Nuclear Route Extinction Factor of Redundant Data Center Entity	99%

applications. The simulation parameters for an evaluation done in three epochs are presented in Table 4. The computing resource utilization is evaluated for the case of communications between the underwater, stratosphere or terrestrial data center. The simulation results obtained as regards the computing resource utilization for the first and

second epochs are presented in Fig. 16 and Fig. 17, respectively.

Evaluation shows that the incorporation of entities in the role of redundant data center entities enhances the compute resource utilization for the contextual computing platform. The contextual computing platform comprises multiple servers across different computing entities. The computing

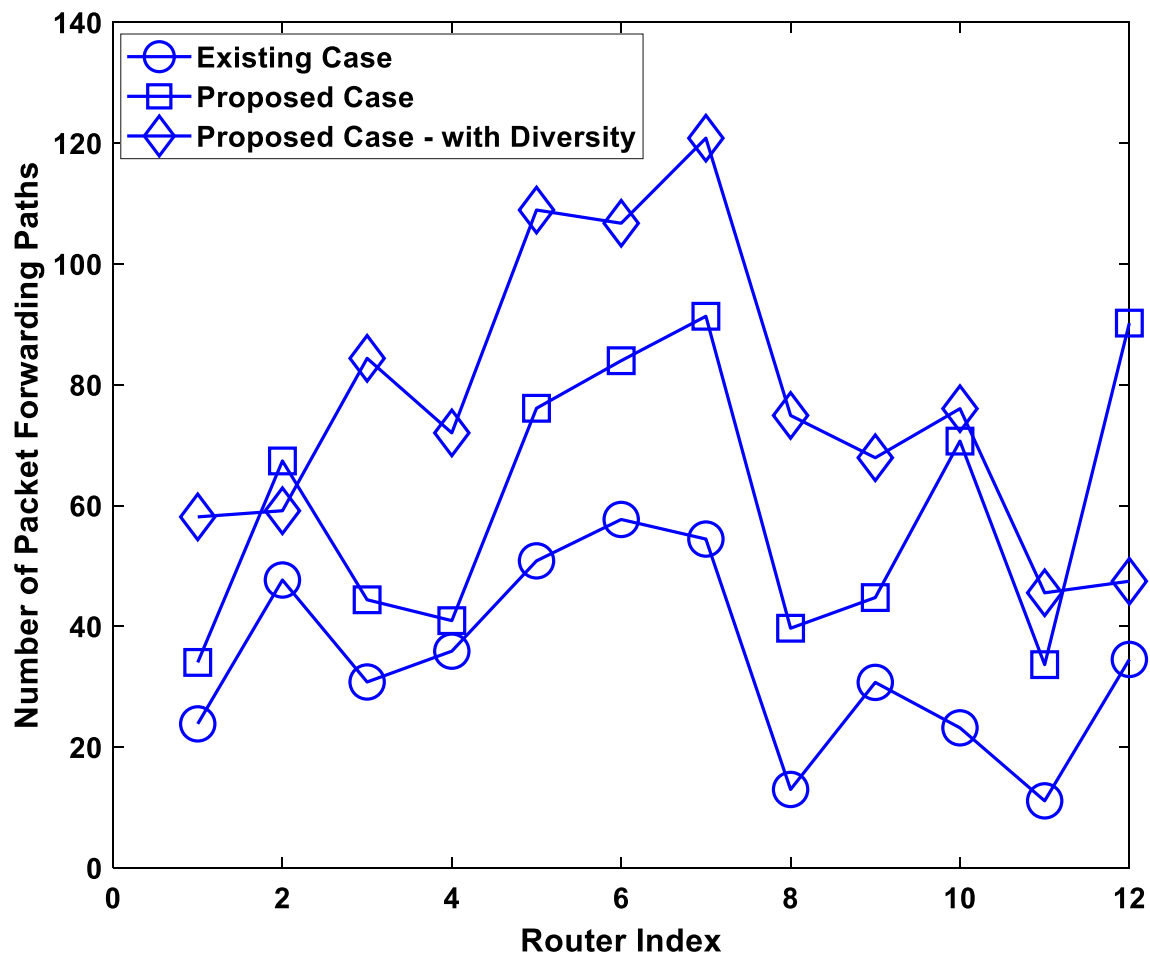


Fig. 18 Results showing the number of packets forwarding paths due to the use of the proposed network architecture in comparison to the existing architecture

entities are the underwater, stratosphere or terrestrial data centers. A high computing resource utilization implies the use of idle computing resources. The results in Figs. 16 and 17 show that the computing resource utilization improves with the incorporation of redundant data center entities. In the first context, the use of the redundant data center entity results in the improvement of the computing resource utilization. For the results in Fig. 16, the inclusion of 1 redundant data center entity in comparison to existing case enhances the computing resource utilization by an average of 23.5%. The use of two redundant data center entities in comparison to the existing case enhances the computing resource utilization by an average of 44.2%. In the first epoch, increasing the number of redundant data center entities by 50% from 1 to 2 enhances computing resource utilization. The computing resource utilization is enhanced by 18.8% on average.

The results in Fig. 17 in the case of the second epoch also show that the proposed mechanism enhances the compute resource utilization. In this case, the use of the proposed network architecture for case comprising 1

redundant data center entity enhances the computing resource utilization by an average of 29.4%. The use of 2 redundant data center entities instead of the existing mechanism enhances the computing resource utilization by an average of 42.4%. Furthermore, an increase in the number of redundant data center entities from 1 to 2 by 50% improves the compute resource utilization by an average of 17%.

C. Performance Evaluation: Number of Packets Forwarding Paths

The performance evaluation examines the number of forwarding paths and its improvement by using the proposed network architecture. The simulation parameters and results are in Table 5, and Fig. 18, respectively. The simulation considers three scenarios. These are Existing Case, Proposed Case and Proposed Case – with diversity. In the existing case, the scenario is one in which the only data center is the underwater data center and is being subjected to missile nuclear attacks. The scenario in the Proposed Case is one in which redundant data center entities are

being used alongside the underwater data center. However, the diversity mechanism and associated architecture are not incorporated in the redundancy enabling network. The scenario in Proposed Case – with diversity is like that presented in Proposed Case but also includes the proposed diversity mechanism and architecture.

As shown, the number of paths varies for each router in the underwater data center or redundant data center entity as signified by the router index. Furthermore, analysis shows that the use of the proposed network architecture with diversity instead of the existing case increases number of packet forwarding paths by 54.7%. The use of the proposed network without diversity instead of existing case increases the number of packets forwarding paths by an average of 41.8%. In addition, an inclusion of the diversity architecture enhances the number of packets forwarding paths by an average of 18.2%.

An increase in the number of packets forwarding paths is beneficial as it provides a means of ensuring the continuity of packet communications. This is applicable to the case of the network architecture incorporating the underwater data center, redundant data center entities and diversity enabling entities.

The results in Fig. 18 show that each router has a varying number of packets forwarding paths. Each of the concerned data center and associated entity experiences missile nuclear attack with varying severities. This implies that each router will have a different number of packets forwarding paths due to the variability in the environment arising from the occurrence of a nuclear missile attack. Nevertheless, the use of the proposed network and the diversity approach enhances the number of packets forwarding paths. The existing case is one where only the underwater data center is being used and experiences nuclear missile attack.

The discussion in this section and the results presented shows that the use of the proposed network architecture improves the network performance. In this case, the network is one that benefits from the use of underwater data centers for information access and data exchange. The presented solution is suitable for the context of a coastal subscriber or subscribers desiring information access at low latency. The concerned coastal subscriber access remote content via the underwater data center. In addition, the concerned coastal region hosts defence base(s) with functional missile bearing submarines. Therefore, the network architecture is suitable for use by a network service provider. The identified network service provider is one that enables subscribers to access remote cloud content via the underwater data center. In this case, the underwater data center is connected to the access mobile terrestrial data network via interfacing network gateways.

7 Conclusion

[Research Findings] The presented research proposes a network architecture suitable for the future internet in a context comprising terrestrial and non-terrestrial data centers. The network architecture is being proposed with the aim of ensuring that nuclear attacks do not lead to a total data center outage. The implied resilience is realized via the design and use of terrestrial and stratosphere data centers to serve as redundant nodes to underwater data centers. In addition, the research formulates a performance model. It also evaluates the performance benefits of using the proposed network architecture. Analysis shows that the use of the proposed network architecture enhances the operational duration of computing platforms in the event of a nuclear attack. Furthermore, the use of the proposed network architecture enhances the computing resource utilization. This enables the support of data storage, processing, and algorithm execution for data driven applications for future internet subscribers. **[Research Limitations]** The research designs a network architecture to support the deployment of underwater data centers in a manner that they are not affected by defense applications. The focus of the research has been on introducing new entities and systems to the communications network. The introduction of complementary capabilities on the submarine is beneficial. However, this requires further research consideration. **[Recommendations for Future Research]** Future research should consider how to incorporate network complementary capabilities to the submarine i.e., defense applications. In addition, the analysis of the research performance has considered the use of mathematical formulation and simulations. Future research should consider the suitability of the use of emulation system approaches. In addition, future work should focus on how to integrate the proposed network architecture. The integration in this case refers to how the proposed network architecture is interfaced with existing network standards.

Acknowledgements The support of the Cape Peninsula University of Technology (Electrical, Electronic and Computer Engineering) is acknowledged.

Author contributions Not applicable.

Funding Open access funding provided by Cape Peninsula University of Technology.

Availability of data and materials All data generated or analyzed during this study are included in the submission.

Declarations

Conflict of interest The author declares that there are no conflicts of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abbasi K et al (2023) Reducing the risks of nuclear war: the role of health professionals. *J Public Health Policy* 44(3):344–347. <https://doi.org/10.1057/s41271-023-00432-7>
- Abbate J (1999) Cold War and White Heat: the origins and meanings of packet switching. In: MacKenzie D, Wajcman J (eds) *Chpater 25 in the social shaping of technology*, 2nd edn. Open University Press, Buckingham
- Alqahtani J, Hamdaoui B (2018) Rethinking fat-tree topology design for cloud data centers. In: 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp 1–6. <https://doi.org/10.1109/GLOCOM.2018.8647774>
- Arbatov A (2020) Nuclear deterrence: a guarantee for or threat to strategic stability? In: *NL ARMS*, pp 65–86. https://doi.org/10.1007/978-94-6265-419-8_5
- Bay M (2017) Conversations with a pioneer: Paul Baran in his own words. *Internet Hist* 1(3):273–282. <https://doi.org/10.1080/24701475.2017.1345469>
- Clark B (2023) The emerging era in undersea warfare. Centre for Strategic and Budgetary Assessments, [Online] [https://csbaonline.org/uploads/documents/CSBA6292_\(Undersea_Warfare_Reprint\)_web.pdf](https://csbaonline.org/uploads/documents/CSBA6292_(Undersea_Warfare_Reprint)_web.pdf)
- Clark D, Field F, Richards M (2023) Computer networks and the internet: a brief history of predicting their future. [Online] <http://groups.csail.mit.edu/ana/People/DDC/Predicting-the-future-3-0.pdf>
- Congressional Research Office (2022) A low-yield, submarine-launched nuclear warhead: overview of the expert debate. [Online] <https://sgp.fas.org/crs/nuke/IF1143.pdf>. Accessed 23 Sep 2022
- Congressional Research Office (2022) Navy Columbia (SSBN – 826) Class Ballistic Missile Submarine Program: Background and Issues for Congress [Online]. <https://sgp.fas.org/crs/weapons/R41129.pdf>. Accessed 23 Sep 2022
- Cutler B, Fowers S, Kramer J, Peterson E (2017) Dunking the data center. *IEEE Spectr* 54(3):26–31. <https://doi.org/10.1109/MSPEC.2017.7864753>
- Das R, Inuwa MM (2023) A review on fog computing: issues, characteristics, challenges, and potential applications. *Telemat Inform Rep* 10:100049. <https://doi.org/10.1016/j.teler.2023.100049>
- Ellison B, Evans D, Lytwyn M, Schwalbe J (2023) Without precedent: global emerging trends in nuclear and hypersonic weapons. <https://nipp.org/wp-content/uploads/2023/03/JHU-Ana-lysis-3.1.pdf>. Accessed 1 Oct 2023
- Ensan M, Joudeh H, Alvarado A, Gustavsson U, Willems FMJ (2021) On cloud radio access networks with cascade oblivious relaying. In: 2021 IEEE Information Theory Workshop (ITW), 2021, pp 1–6. <https://doi.org/10.1109/ITW48936.2021.9611433>
- Fink A (2023) The Wind Rose's Directions: Russia's Strategic Deterrence during the First Year of the War in Ukraine. https://www.ifri.org/sites/default/files/atoms/files/ifri_fink_russian_strategic_deterrence_aout2023.pdf
- Gale RP, Hochhaus A (2023) Nuclear war and physicians' social responsibility. *Leukemia*. <https://doi.org/10.1038/s41375-023-02025-5>
- Grossi RM (2022) Nuclear law: the global debate. *Nuclear Law*. https://doi.org/10.1007/978-94-6265-495-2_1
- Guo C, Lu G, Li D, Wu H, Zhang X, Shi Y, Tian C, Zhang Y, Lu S (2009) BCube. *ACM SIGCOMM Comput Commun Rev* 39(4):63–74. <https://doi.org/10.1145/1594977.1592577>
- Hiroshima for Global Peace Plan, Hiroshima Report (2018) Evaluation of Achievement in Nuclear Disarmament, Non-Proliferation and Nuclear Security in 2017', Center for the promotion of disarmament and non – proliferation: The Japan Institute of International Affairs
- Hu Z-H, Zheng Y-X, Wang Y-G (2022) Packing computing servers into the vessel of an underwater data center considering cooling efficiency. *Appl Energy* 314:118986. <https://doi.org/10.1016/j.apenergy.2022.118986>
- Johnson J (2023) Post-9/11 US thinking and approaches to nuclear deterrence: the Bush Doctrine and the role of nuclear weapons in US deterrence strategy. <https://doi.org/10.1057/s41311-023-00485-1>
- Kazys R, Sliteris R, Rekuviene R, Zukauskas E, Mazeika L (2015) Ultrasonic technique for density measurement of liquids in extreme conditions. *Sensors* 15(8):19393–19415. <https://doi.org/10.3390/s150819393>
- Kirchberger S (2023) China's pursuit of defense technologies: implications for U.S. and Multilateral Export Control and Investment Screening Regimes' China's Undersea Warfare. [Online]. https://www.uscc.gov/sites/default/files/2023-04/Sarah_Kirchberger_Testimony.pdf. Accessed 1 Oct 2023
- Kliks A, Musznicki B, Kowalik K, Kryszkiewicz P (2017) Perspectives for resource sharing in 5G networks. *Telecommun Syst* 68(4):605–619. <https://doi.org/10.1007/s11235-017-0411-3>
- Kristensen HM, Korda M (2019) French nuclear forces, 2019. *Bull at Sci* 75(1):51–55. <https://doi.org/10.1080/00963402.2019.1556003>
- Kristensen HM, Korda M (2023) United States nuclear weapons, 2023. *Bull at Sci* 79(1):28–52. <https://doi.org/10.1080/00963402.2022.2156686>
- Kristensen HM, Korda M, Johns E (2023) French nuclear weapons, 2023. *Bull at Sci* 79(4):272–281. <https://doi.org/10.1080/00963402.2023.2223088>
- Kristensen HM, Korda M, Johns E (2023) Pakistan nuclear weapons, 2023. *Bulletin of the Atomic Scientists*. <https://thebulletin.org/premium/2023-09/pakistan-nuclear-weapons-2023/>. Accessed 1 Oct 2023
- Lamberti NA et al (2015) A resonant sensor for liquid density measurement based on a piezoelectric bimorph. N: 2015 IEEE International Ultrasonics Symposium (IUS), 2015, pp 1–4. <https://doi.org/10.1109/ULTSYM.2015.0536>
- Lanin DG (2023) Topical issues of the introduction of artificial intelligence into the design process of nuclear power plants. *Power Technol Eng*. <https://doi.org/10.1007/s10749-023-01612-x>
- Leslie C (2013) Competing histories of technology: recognizing the vital role of international scientific communities behind the innovation of the internet. In: *Making the history of computing relevant*, pp.196–206. https://doi.org/10.1007/978-3-642-41650-7_18
- Lin D, Liu Y, Hamdi M, Muppala J (2012) Hyper-BCube: a scalable data center network. In: 2012 IEEE International Conference on

- Communications (ICC), Ottawa, ON, Canada, 2012, pp. 2918–2923, <https://doi.org/10.1109/ICC.2012.6363759>.
- Lingshu L, Jiangxing W, Hongchao H, Wenyan L, Zehua G (2021) Secure cloud architecture for 5G core network. *Chin J Electron* 30(3):516–522. <https://doi.org/10.1049/cje.2021.04.005>
- Periola AA (2020) Aerial computing—security from missile threats and enhancing PUE. *Aerospace Systems* 3(4):327–342. <https://doi.org/10.1007/s42401-020-00064-9>
- Peters J (2021) Below the surface: undersea warfare challenges in the 21st century. In: *From the North Atlantic to the South China Sea*, pp 93–110, <https://doi.org/10.5771/9783748921011-93>.
- Ridley P, Fontan J, Corke P (2022) Submarine dynamic modelling. [Online] <https://core.ac.uk/download/pdf/10898542.pdf>. Accessed 23 Sep 2022
- Ruff TA (2022) Ending nuclear weapons before they end us: current challenges and paths to avoiding a public health catastrophe. *J Public Health Policy* 43(1):5–17. <https://doi.org/10.1057/s41271-021-00331-9>
- Saba T, Rehman A, Haseeb K, Alam T, Jeon G (2023) Cloud-edge load balancing distributed protocol for IoE services using swarm intelligence. *Clust Comput*. <https://doi.org/10.1007/s10586-022-03916-5>
- Uchida H, Kayukawa Y, Maeda Y (2019) Ultra high-resolution seawater density sensor based on a refractive index measurement using the spectroscopic interference method. *Sci Rep* 9(1):10. <https://doi.org/10.1038/s41598-019-52020-z>
- van Hooft P (2020) The US and Extended Deterrence. In: *NL ARMS*, pp 87–107, https://doi.org/10.1007/978-94-6265-419-8_6.
- Wen J, Chen Z, Jin X, Liu X (2023) Rise of the planet of serverless computing: a systematic review. *ACM Trans Softw Eng Methodol*. <https://doi.org/10.1145/3579643>
- Won S, Lee C (2020) Simulation of the mushroom cloud generated from a high-energy explosion using large-eddy simulation. *J Mech Sci Technol* 34(6):2443–2453. <https://doi.org/10.1007/s12206-020-0520-x>
- Zhao T (2022) Tides of change: China’s nuclear ballistic missile submarines and strategic stability. *Carnegie Endowment for International Peace* [Online] https://carnegieendowment.org/files/Zhao_SSBN_final.pdf. Accessed 23 Sep 2022

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.