Joint Energy and Security Optimization in Underwater Wireless Communication Networks

Kazi Yasin Islam, *Member, IEEE*, Iftekhar Ahmad, *Member, IEEE*, Yue Rong, *Senior Member, IEEE*, and Daryoush Habibi, *Senior Member, IEEE*

***Abstract*—Underwater wireless communication networks (UWCNs) can support a wide range of applications in the underwater domain, including mining and drilling, coastline monitoring, border surveillance, and submarine/mine detection. Some of these applications are sensitive in nature (e.g., military) and demand stringent security requirements for data communications. In order to prevent malicious attacks (e.g., jamming) in these UWCNs, robust security countermeasures must be implemented. Additionally, sensitive data communications must be protected. However, computationally expensive security protocols, such as encryption, can severely shorten UWCN lifetime, where battery-powered nodes already suffer from scarce energy supplies. In this work, we exploit content caching as a countermeasure for jamming and utilize selective encryption of sensitive data to simultaneously maximize network security and node residual energy in UWCNs. Our work formulates the joint security and residual energy maximization challenge as an optimization problem in which results indicate that the proposed technique can guarantee secure communications without sacrificing network lifespan.**

***Index Terms*—Content caching, encryption, green communications, optimization, security, trust model, underwater wireless communication networks (UWCNs).**

I. Introduction

RADIO-BASED wireless communication networks are vulnerable to various security threats due to the inherent broadcast nature of wireless channels and the heterogeneity of network nodes. In these networks, resource-constrained characteristics, such as limited computational capacity and scarcity of energy supply, accentuate this problem [1]. The security issue is even more pronounced in underwater wireless communication networks (UWCNs) because they suffer from harsher communication environments and additional challenges, such as node mobility/drift, which aggravate the vulnerability of these networks. However, UWCNs are becoming increasingly popular because they have important applications within military, scientific, and industrial [2] domains. For instance, within defence, UWCNs can support diver-to-diver and diver-to-surface platform communications, border monitoring and control, underwater surveillance and reconnaissance, as well as submarine communications. In research, UWCNs facilitate studies of water properties (e.g., temperature, pH, salinity, pressure, and oxygen), aquatic lifeforms, marine ecology, underwater bathymetry, volcanoes, and tsunami dynamics. Furthermore, UWCNs are extensively used by commercial and industrial enterprises to explore oil and gas reservoirs, extract natural resources, monitor underwater pipelines, and cultivate fish [3].

Due to these promising applications of UWCNs across multiple disciplines, it is vital that UWCNs maintain a high standard of security to protect communications. To this end, several works in the literature have addressed the security aspect of UWCNs in an attempt to identify security threats and propose countermeasures to mitigate/thwart them. Domingo et al. [4] have identified key differences between terrestrial sensor networks and UWCNs, focusing on the security aspects of the latter. They have described various attack types, including jammming, wormhole, sinkhole, spoofing, flooding, and sybil attack along with countermeasures, such as authentication and time synchronization for secure underwater communications. The work in [5] has provided a layer-by-layer description of secure communication protocols and has discussed open research issues in the relevant domain. Lal et al. [6] have proposed various approaches, such as node cooperation, context-aware and software-defined networking, as well as adaptive trust and reputation models to improve existing frameworks and to envision novel security protocols in UWCNs. The work in [7] reviews existing works on underwater security challenges and feasible security techniques. A comprehensive survey on UWCN security has been provided in [1] which has discussed in detail the fundamentals of network security, network threats from the physical to transport layer and countermeasures to relevant threats in UWCNs.

Besides these surveys, a flurry of studies has addressed specific security issues in UWCNs. For instance, a synergestic trust model based on support vector machines (SVMs) has been proposed in [8]. Further, an energy-balanced trust cloud migration scheme (ETCM) has been proposed in [9]. Using blockchain technology, a decentralized authentication mechanism has been proposed in [10]. A secure energy-efficient cooperative routing protocol has been proposed in [11]. An optimization framework has been developed to analyze the effects of multipath routing, packet duplication, encryption,

Manuscript received 3 November 2023; accepted 4 December 2023. Date of publication 7 December 2023; date of current version 9 April 2024. *(Corresponding author: Kazi Yasin Islam.)*

Kazi Yasin Islam, Iftekhar Ahmad, and Daryoush Habibi are with the School of Engineering, Edith Cowan University, Perth, WA 6027, Australia (e-mail: kyislam@our.ecu.edu.au; i.ahmad@ecu.edu.au; d.habibi@ecu.edu.au).

Yue Rong is with the School of Electrical Engineering, Computing and Mathematical Sciences, Curtin University, Bentley, WA 6102, Australia (e-mail: y.rong@curtin.edu.au).

Digital Object Identifier 10.1109/JIOT.2023.3340269

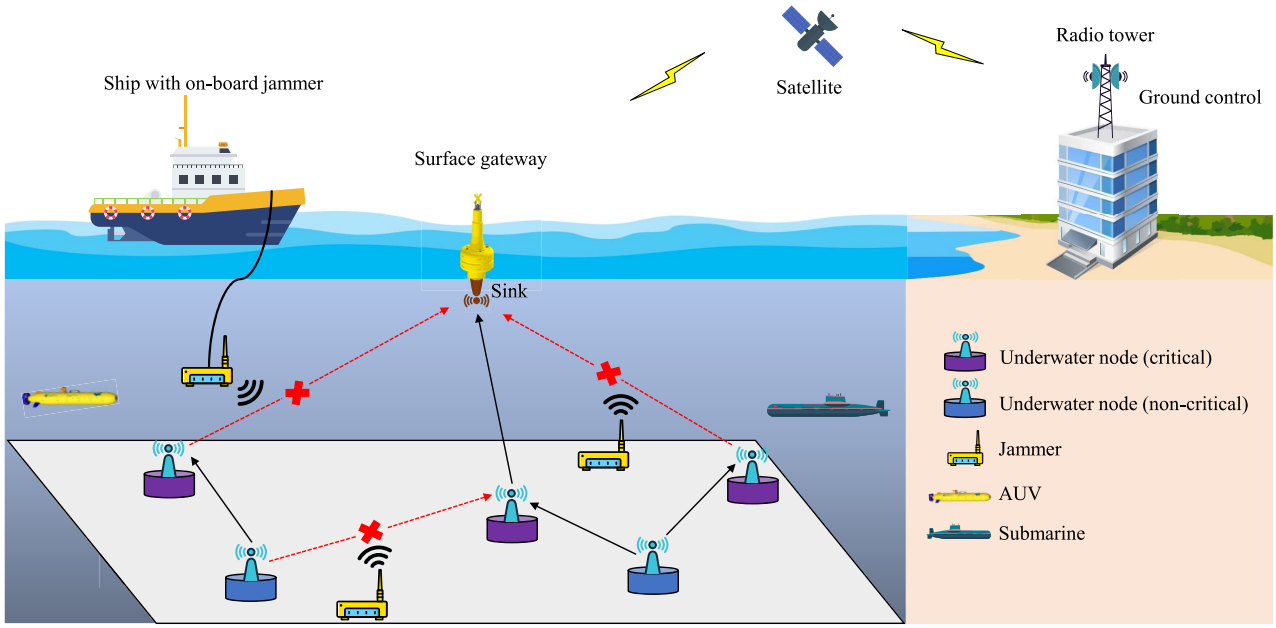


Fig. 1. UWCN with jammed communications.

and data fragmentation on UWCN lifetime in [12]. As a countermeasure for eavesdropping attacks, the work in [13] has proposed a strategy to optimize the power required to maximize the secrecy sum rate of a full-duplex relay-assisted nonorthogonal multiple access UWCN.

Many works have also attempted to address jamming in UWCNs. The work in [14] has utilized game theory to conduct an analysis of jamming attacks in UWCNs, where sensors and jammers are allowed to play jamming games. In this way, each sensor can select its transmit power when an interfering signal is present, and optimize its signal-to-interference and noise ratio (SINR) and transmission costs. A deep Q-networks (DQNs)-based anti-jamming mechanism that controls transmit power and leverages transducer mobility has been proposed in [15]. This technique can reduce the bit error rate (BER) and improve SINR against reactive jamming as compared to other Q-learning-based techniques. A similar approach has been undertaken in [16], where a deep reinforcement learning (RL)-based jamming countermeasure that optimizes relay node mobility and power allocation without knowledge of channel and jamming model has been proposed. Similar to [15], this technique saves power, reduces BER, and improves utility of relay nodes against the established benchmark. More recently, a game-theoretic approach, with the jammer and the sensor node set as players in a multistage game has been proposed in [17], where each derives optimal strategies for their respective purposes (i.e., jamming and transmitting data, respectively).

To the best of our knowledge, although these relevant works in the literature offer jamming mitigation techniques, none have investigated the effect of caching as a countermeasure for jamming. Moreover, no work has investigated the optimization of total network trust and residual energy in an effort to maximize network security and lifetime and study its effects on salient network parameters, such as power consumption, trust metrics, and traffic serviced. Additionally, no work has also addressed selective encryption of sensitive data to simultaneously improve the secrecy of communication and save energy in UWCNs.

Our work, therefore, is the first major study investigating the optimization of network security from a trust and residual power perspective by leveraging the technique of content caching and selectively encrypting data. The main contributions of this work are summarized as follows.

1) We develop an optimization model that jointly maximizes UWCN trust and total residual energy. This optimization model exploits: a) a content caching mechanism during jamming attacks and b) selective encryption of sensitive data traversing the network.
2) We solve the optimization problem and conduct a performance evaluation across two scenarios: Scenario I), jamming attacks on UWCN with three levels of jamming—low, medium, and high; and Scenario II), transmission of two types of data—nonsensitive and sensitive.
3) We compare and contrast the performance of our proposed solution against the existing solution and investigate the effects of both on network metrics, such as power consumption, trust, and traffic delivery. Our results indicate that the proposed solution outperforms the existing solution by offering lower power consumption, higher trust, and better traffic delivery, with an overall better yield of the objective function that maximizes network trust and residual energy.

II. Problem Description

A 3-D UWCN architecture is presented in Fig. 1. This UWCN consists of several underwater nodes that are classified into critical and noncritical nodes. Critical nodes are

those whose battery depletion affects the availability of the entire UWCN. In contrast, noncritical nodes are those whose battery depletion does not compromise the availability of the UWCN [18]. The network also includes jamming nodes that can be submerged from vessels or can be placed on seabeds in the vicinity of network nodes.

The nature of jamming can be random or periodic. According to [19], random jamming is when jamming signals are sent for random periods and then switched off for the rest of the time. Periodic jamming is a subset of random jamming where jamming occurs with specific duty cycles. Often, jammers can periodically transmit jamming signals with a specific duty cycle (i.e., periodic jamming) to match and interrupt the regular periodic messaging schedule of underwater nodes.

As noted in [17], a network jammer has a twofold objective—the first is to disrupt network communications and the second is to reduce network lifetime by forcing multiple retransmissions from network nodes.

Given the scenario in Fig. 1, one key research question can be formulated as "*How can UWC network security be improved, and, at the same time, network energy consumption be reduced in the presence of jamming attacks, while ensuring the integrity of sensitive data transmissions*"?

To answer this question, we formulate the network security challenge as an optimization problem that utilizes content-caching as a technique to mitigate the effects of jamming. Moreover, the proposed optimization problem decides which content should be encrypted based on the sensitivity of data and the security status of a link. To evaluate the efficacy of our solution, we introduce periodic jamming in the network during data transmission and observe the effects of jamming on salient network parameters, such as energy consumption, traffic received, and overall network security in terms of node trust and link trust. We also transmit sensitive data through both secure and unsecure links and observe its effects on the aforementioned parameters.

It is important to note that the focus of this work is to mitigate the effects of jamming. It is not a preventative measure but a reactive one. The solution is designed to work against any type of jamming and therefore jamming prediction is not required.

The proposed content-caching technique stores data until the jamming attack is over. In this way, our proposed technique is expected to reduce the number of retransmissions, hence saving energy and simultaneously improving the probability of successful data transmission.

In addition to caching to mitigate jamming, the special treatment of sensitive data transmission (e.g., mission-critical data transmission for underwater surveillance) by our proposed strategy is expected to ensure that data is transmitted in a secure way and at a lower energy expense, simultaneously.

Sensitive data transmission (e.g., defence applications) must be encrypted to protect data from eavesdropping or man-in-the-middle attacks. Nonsensitive data transmissions (e.g., for scientific exploration projects), however, need not be classified. The sensitivity of data transmission can be predetermined depending on the application domain.

Although some applications are delay-sensitive, others are delay-tolerant (e.g., collection of environmental data). Our proposed strategy also ensures that the end-to-end latency is properly managed for delay-sensitive applications.

III. System Model

In this section, we introduce our underwater channel model (Section III-A), underwater energy model (Section III-B), underwater trust model (Section III-C), underwater network model (Section III-D), and the proposed mixed-integer programming (MIP) model (Section III-E).

A. Underwater Channel Model

We consider a UWCN where nodes are equipped with heterogeneous multimodal communication capabilities. Nodes are equipped with both acoustic and optical modems. Communication modes can switch between acoustic and optical forms depending on channel conditions and traffic demands.

At first, we develop the acoustic channel model. The acoustic signal-to-noise ratio (SNR) at the receiver is given by the ratio of received acoustic power P_{ac}^{r} to the acoustic ambient noise power spectral density (PSD) $(NL)_{ac,\text{total}}$ and the noise bandwidth of the acoustic receiver (B_{ac}) as [20]

$$\xi_{ac} = P_{ac}^{r} / \left(L_{ac} \cdot (NL)_{ac,\text{total}} \cdot B_{ac}\right). \tag{1}$$

The acoustic path loss in (1) L_{ac} is given by [21]

$$L_{ac} = l^{\kappa} \cdot \alpha(f)^{l \cdot 10^{-3}} \cdot A_0 \tag{2}$$

where l^{κ} denotes the spreading loss over a distance l (m); the path-loss exponent κ can take a value of 1 for cylindrical, 2 for spherical, and 1.5 for "practical" spreading; and A_0 denotes a unit normalization factor incorporating fixed losses [22].

$\alpha(f)$ in (2) denotes the absorption coefficient (dB/km) that can be expressed empirically using the Francois and Garrison [23], [24] model that encapsulates oceanographic factors within the frequency range 100 Hz $< f <$ 1 MHz, and is given by

$$\alpha(f) = \frac{A_1 P_1 f_1 f^2}{f^2 + f_1^2} + \frac{A_2 P_2 f_2 f^2}{f^2 + f_2^2} + A_3 P_3 f^2 \tag{3}$$

where the first term describes the ionic relaxation effects caused by the presence of boric acid (H_3BO_3) molecules, the second term describes the effects due to the magnesium sulfate ($MgSO_4$) salt concentration, and the third term describes the viscous absorption component due to pure water.

In the first term of (3), A_1 is the boric acid component, P_1 is the depth pressure resulting from A_1, and f_1 is the relaxation frequency for the boric acid component in seawater and are given, respectively, as

$$A_1 = \frac{8.68}{c} \times 10^{(0.78 \text{ pH} - 5)} \tag{4}$$

$$P_1 = 1 \tag{5}$$

$$f_1 = 2.8\sqrt{\frac{S}{35}} \times 10^{(4 - 1245/(273+T))} \tag{6}$$

where c is the underwater sound speed (m/s), pH is the water pH, S is salinity [parts per thousand (PPTs)], and T is temperature (°C).

In the second term, A_2 is the magnesium sulfate component, P_2 is the depth pressure resulting from A_2, and f_2 is the relaxation frequency for the magnesium sulfate component in seawater. They can be expressed, respectively, as

$$A_2 = 21.44\left(\frac{S}{c}\right) \times (1 + 0.025T) \tag{7}$$

$$P_2 = 1 - 1.37 \times 10^{-4} z + 6.2 \times 10^{-9} z^2 \tag{8}$$

$$f_2 = \frac{8.17 \times 10^{(8-1990/(273+T))}}{1 + 0.0018(S-35)} \tag{9}$$

where z is the water depth.

Finally, in the third term, A_3 is the pure water viscosity component (dB km $^{-1}$ kHz^2), and P_3 is the depth pressure resulting from A_3, and they are given by

$$A_3 = \begin{cases} 4.937 \times 10^{-4} - 2.59 \times 10^{-5} T \\ + 9.11 \times 10^{-7} T^2 - 1.5 \times 10^{-8} T^3 \\ \text{for } T \leq 20^\circ \text{ C} \end{cases} \tag{10a}$$

$$\begin{cases} 3.964 \times 10^{-4} - 1.146 \times 10^{-5} T \\ + 1.45 \times 10^{-7} T^2 - 6.65 \times 10^{-10} T^3 \\ \text{for } T > 20^\circ \text{ C} \end{cases} \tag{10b}$$

$$P_3 = 1 - 3.83 \times 10^{-5} z + 4.9 \times 10^{-10} z^2. \tag{11}$$

In the channel model, the overall PSD of the ambient noise $(NL)_{ac,\text{total}}$ is given by [20], [25], [26], [27]

$$\begin{aligned} (NL)_{ac,\text{total}} = {} & \overbrace{10^{(17-30\log f)\ /10}}^{(NL)_t} \\ & + \overbrace{10^{(40+20(s-0.5)+26\log f-60\log(f+0.03))/10}}^{(NL)_s} \\ & + \overbrace{10^{(50+7.5\sqrt{w}+20\log f-40\log(f+0.4))/10}}^{(NL)_w} \\ & + \overbrace{10^{(-15+20\log f)/10}}^{(NL)_{\text{th}}} \end{aligned} \tag{12}$$

where noise component $(NL)_t$ is the noise due to oceanic wave turbulence; $(NL)_s$ is the noise due to shipping/vessel activities on water; $(NL)_w$ is the noise generated by waves; and $(NL)_{\text{th}}$ is the noise due to thermal agitation caused by oceanic pressure fluctuations. $s \in [0, 1]$ in $(NL)_s$ is the shipping activity factor, where 0 and 1 indicate low and high shipping activity, respectively. w in $(NL)_w$ is the wind speed in m/s.

Another common noise source in underwater environments is impulsive noise due to human activities (e.g., pile driving in the harbor) and natural sources (e.g., seismic activities). Impulsive noise depends on the deployment environment, is usually sparse, can be suppressed through receiver design [28], and mainly encountered in port areas [29]. Although impulsive noise can be detrimental, our proposed solution can still be functional in its presence as it can be treated as an undesired signal such as jamming.

For a given traffic load C (Mb/s) and acoustic link bandwidth B_{ac} (kHz), an acoustic link must meet the threshold SNR

$$\xi_{ac}^{TH} = 2^{C/B_{ac}} - 1. \tag{13}$$

The received signal power P_{ac}^r is given by the transmit acoustic power and the acoustic path loss L_{ac} as

$$P_{ac}^r = P_{ac}^t \cdot L_{ac}^{-1}. \tag{14}$$

Then, equating (1) and (13), substituting (14) in (1), and rearranging (1), the acoustic transmit power is formulated as

$$P_{ac}^t = \xi_{ac}^{TH} \cdot L_{ac} \cdot (NL)_{ac,\text{total}} \cdot B_{ac}. \tag{15}$$

Similar to acoustic power, optical transmit power can be derived and expressed as a function of target/threshold optical SNR ξ_{op}^{TH}, underwater optical channel loss L_{op}, underwater optical noise $\Delta_{op,\text{total}}$, and the photodetector responsivity of the optical receiver ρ as

$$P_{op}^t = \left(\sqrt{\xi_{op}^{TH}} \cdot \Delta_{op,\text{total}}\right) / \left(L_{op} \cdot \rho\right). \tag{16}$$

Here, the optical channel attenuation L_{op} is given as [30]

$$\begin{aligned} L_{op} = {} & \chi^2 \cdot \left((A_r \cdot n_t \cdot n_r \cdot \cos\theta) / \left(2\pi \cdot l^2 (1 - \cos\theta_0)\right)\right) \\ & \cdot \exp(-c(\lambda) \cdot l) \end{aligned} \tag{17}$$

where χ^2 is the optical fading amplitude for weak turbulence in water, A_r denotes the aperture of the optical receiver; n_t and n_r represent transmitter and receiver efficiencies, respectively; the angle of inclination from the transmitter to the receiver is denoted by θ; and the divergence angle of the transmitter beam is given by θ_0.

The term $\exp(-c(\lambda) \cdot l)$ is the optical propagation loss factor, where $c(\lambda)$ is the underwater optical beam extinction coefficient (i.e., a function of optical wavelength λ), which indicates the amount of absorption and scattering in the optical beam [31], [32].

The total optical noise is modeled as additive white Gaussian noise (AWGN) with zero mean and variance [30], which can be expressed as

$$\begin{aligned} \Delta_{op,\text{total}}^2 = {} & \overbrace{(4k_B \cdot T_e \cdot F \cdot B)\ /R_L}^{\delta_{TH}^2} + \overbrace{2q \cdot I_{DC} \cdot B}^{\delta_{DC}^2} \\ & + \overbrace{2q \cdot \rho \cdot P_i \cdot B}^{\delta_{SS}^2} + \overbrace{2q \cdot \rho \cdot P_{BG} \cdot B}^{\delta_{BG}^2} \end{aligned} \tag{18}$$

where δ_{TH}^2 is the thermal/Johnson noise, δ_{DC}^2 is the dark current noise, δ_{SS}^2 is the quantum/signal shot noise, and δ_{BG}^2 is the background noise.

Moreover in (18), k_B denotes the Boltzmann constant, T_e represents the equivalent temperature, F denotes the system noise figure, B is the electronic bandwidth, and R_L is the receiver load resistance. Further, q is the charge of an electron, I_{DC} is the reverse leakage current of a photodiode, ρ is the receiver photodiode's responsivity, and P_i is the optical power from the light-of-interest received by the receiver.

TABLE I
PARAMETERS USED IN ANALYSIS

Symbol	Parameter	Value	Symbol	Parameter	Value
l	Transmission distance	1-100 m	A_r	Optical receiver aperture	0.01 m^2
κ	Acoustic path loss exponent	1.5	n_r	Optical receiver efficiency	0.9
s	Shipping activity factor	0.5	n_t	Optical transmitter efficiency	0.9
w	Speed of wind	10 m/s	θ	Angle of inclination between transmitter & receiver	10°
B_{ac}	Acoustic receiver narrow bandwidth	5 kHz	k_B	Boltzmann constant	1.38×10^{-23} J/K
θ_0	Angle of divergence for optical beam	10°	F	System noise figure	4
T_e	Equivalent temperature	290 K	R_L	Load resistance	100 Ω
B	Electronic noise bandwidth	5 MHz	I_{DC}	Dark current in photo-diode	1.23×10^{-9} A
q	Charge of an electron	1.602×10^{-19} C	FOV	Optical field-of-view at receiver	10°
ρ	Photo-diode responsivity	386 μA/W	T_F	Optical filter transmissivity	0.95
μ	Bandwidth of optical filter at receiver	30 nm	v	Velocity of light underwater	2.25×10^8 m/s
h	Planck's constant	6.62×10^{-34} m^2 kg/s	τ_0	Atmospheric transmission	0.37
α	Radiant absorption factor	0.5			

Additionally, P_{BG} represents underwater background noise power, which is composed of P_{solar} and $P_{\text{blackbody}}$ and can be written as [33]

$$P_{\text{BG}} = \overbrace{L_{\text{solar}} \cdot \pi (\text{FOV})^2 \cdot A_r \cdot \mu \cdot T_F}^{P_{\text{solar}}} + \overbrace{2hv^2\alpha \cdot T_A \cdot (P_{\text{solar}}/L_{\text{solar}})}^{P_{\text{blackbody}}} \cdot 1 \Big/ \left(\lambda^5 \cdot \left[\exp\left(\frac{hv}{\lambda k_B T_e}\right) - 1\right]\right) \tag{19}$$

where L_{solar} represents solar radiance, FOV is the field of view of the optical receiver, μ represents the optical receiver's filter bandwidth, T_F denotes the optical transmissivity, h is the Planck constant, v represents the underwater speed of light, α denotes the radiant absorption factor, and T_A is the transmission in water ($T_A = \exp(-\tau_0)$, where τ_0 is the atmospheric transmission).

Table I summarizes all parameter settings and presents the list of symbols and notations used in this article.

B. Underwater Energy Model

The total power consumption of a multimodal UWC node can be given as

$$P_{\text{cons}} = P^t_{ac} + P^t_{op} + P^r_{ac} + P^r_{op} + P_{\text{proc}} + P_{\text{idle}} \tag{20}$$

where P^t_{ac} and P^t_{op} are acoustic and optical transmit powers, respectively; P^r_{ac} and P^r_{op} are acoustic and optical receive powers, respectively; and P_{proc} and P_{idle} are power consumption due to signal processing and maintaining node idle states, respectively. For the acoustic component, power consumption configurations of Woods Hole Oceanographic Institute (WHOI) acoustic micromodem [34] were used. For the optical component, power consumption specifications of LUMA 100 [35] were used. The power consumption figures for each are presented in Table II.

Equation (20) can be simplified as

$$P_{\text{cons}} = P_{tx} + P_{rx} + P_{\text{proc}} + P_{\text{idle}} \tag{21}$$

where P_{tx} and P_{rx} denote transmit and receive power, respectively.

Given a transmission lasts for t seconds, the total node energy consumption is written as

$$E_{\text{node}} = \left(P_t + P_r + P_{\text{proc}} + P_{\text{idle}}\right) \times t \tag{22}$$

In our study, we consider two different types of transmissions—encrypted and nonencrypted—leading to two

TABLE II
POWER CONSUMPTION SPECIFICATIONS

Modem	Transmit (W)	Receive (W)	Process (W)	Idle (W)
WHOI Micromodem (Standard)	60	0.79	0.5	0.790
LUMA 100	5	2.00	0.2	0.003

different types of link energy consumption. This is given by

$$E_{\text{link}} = \begin{cases} E_{\text{link},e}, & \text{if encryption is required, and} \\ E_{\text{link},ne}, & \text{if no encryption is required.} \end{cases} \tag{23}$$

The total energy consumption, which is expressed in Section III-E, is the summation of node energy consumption and link energy consumption.

C. Underwater Trust Model

Node trust $\mathcal{N}$ is a function of node honesty (NH) and node competence (NC) and is given by [5]

$$\mathcal{N} = \begin{cases} 0.5 + (\text{NH} - 0.5) \times \text{NC}, & \text{if NH} \geq 0.5 \\ \text{NH} \times \text{NC}, & \text{otherwise.} \end{cases} \tag{24}$$

Link trust $\mathcal{L}$ is dependent on link quality (LQ) and link capacity (LC) and is given by [5]

$$\mathcal{L} = \begin{cases} 0.5 + (\text{LQ} - 0.5) \times \text{LC}, & \text{if LQ} \leq 0.5 \\ \text{LQ} \times \text{LC}, & \text{otherwise.} \end{cases} \tag{25}$$

The total trust, which is expressed in Section III-E, is the summation of node trust and link trust. The calculation of the parameters NH, NC, and LQ is beyond the scope of this work, and their parametric values have been generated as random numbers between 0 and 1.

D. Underwater Network Model

A UWCN composed of several sensor nodes and one sink node is illustrated in Fig. 1. There are a total of $|\boldsymbol{U}| = |\boldsymbol{V}| + 1$ nodes in the UWCN where there are $|\boldsymbol{U}|$ $(v = 1, 2, \ldots, |\boldsymbol{V}|)$ sensor nodes with one sink node. $|\boldsymbol{U}|$ indicates the cardinality of the set $\boldsymbol{U}$ containing all nodes, whereas $|\boldsymbol{V}|$ indicates the cardinality of the set $\boldsymbol{V}$ containing all sensor nodes. The subset of critical nodes (i.e., nodes whose failure can disrupt the entire network) is given by $\boldsymbol{C} \subseteq \boldsymbol{V}$, and that of noncritical nodes (i.e., any node that is not critical) is given by $\boldsymbol{D} \subseteq \boldsymbol{V}$, respectively.

All the sets considered to formulate the network model are given as follows.

1) $\boldsymbol{E}$: Set of links.
2) $\boldsymbol{U}$: Set of all nodes.
3) $\boldsymbol{V}$: Set of sensor nodes (subset of $\boldsymbol{U}$).
4) $\boldsymbol{J}$: Set of jammed nodes (subset of $\boldsymbol{U}$).
5) $\boldsymbol{K}$: Set of network flows.
6) $\boldsymbol{C}$: Set of critical nodes (subset of $\boldsymbol{V}$).
7) $\boldsymbol{D}$: Set of noncritical nodes (subset of $\boldsymbol{V}$).

A directed, weighted graph $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$, consisting of $\boldsymbol{V}$ vertices and $\boldsymbol{E}$ edges/links, is used in the formulation of the optimization problem. In this model, i represents source nodes and j represents destination nodes. In the graph, each link $(i, j) \in \boldsymbol{E}$ has a capacity limit of $u_{ij} \geq 0$. Additionally, traffic demand $k \in \boldsymbol{K}$ sends traffic of the volume b^k from the source node(s) $s(k)$ to the destination node(s) $d(k)$. Traversal of traffic occurs through transshipment node(s) $t(k)$ if relay nodes are used.

The set $r = \{1, \ldots, N_r\}$ is an index set of the set of links $\boldsymbol{E}$, which is utilized to identify possible routes for each ith node to the sink/surface gateway. Each route r is determined by the optimization model. Therefore, the set of routes r is not predefined, but determined by solving the optimization model.

There are 19 nodes in the network deployed at different depths within an underwater area of 1000 m by 1000 m. These nodes are arranged in ring, star, and tree topologies, similar to the work in [36].

The traffic model used in this work was based on a number of Internet of Underwater Things (IoUT) applications, as described in various studies in [2], [37], [38], and [39]. The traffic types include constant bit rate (CBR), variable bit rate (VBR), and best effort (BE) traffic, evaluated at hourly intervals to capture underwater traffic fluctuations. The scope of our study includes both low- and high-data-rate traffic demands in underwater environments. Among low-data-rate applications are scientific measurements of temperature, pH, and salinity using underwater sensors. As for the high data rate applications, real-time, high-resolution image and/or video transfer by AUVs were considered.

E. MIP Model

The decision variables to formulate the MIP model are as follows.

1) $x_{i,j}^{k,r}$: A positive continuous decision variable that models the kth traffic flow over the link (i, j) on the rth route.
2) a_i^k: A binary decision variable taking 1 if the kth traffic flows through node i, and 0 otherwise.
3) $\zeta_{i,j}^{k,r}$: A binary decision variable taking 1 if the kth traffic flowing over the link (i, j) is encrypted, and 0 otherwise.

Node trust for the ith node is given by

$$NT_i = \mathcal{N}_i \times a_i^k. \tag{26}$$

Link trust for the ith link is given by

$$LT_i = \mathcal{L}_i \times x_{i,j}^{k,r}. \tag{27}$$

Node energy for the ith node is calculated by

$$E_{i,\text{node}} = E_{\text{node}} \times a_i^k. \tag{28}$$

Link energy for the ith link is given by

$$E_{i,\text{link}} = \left(E_{\text{link},e} \times x_{i,j}^{k,r} \times \zeta_{i,j}^{k,r}\right) + \left(E_{\text{link},ne} \times x_{i,j}^{k,r} \times \left(1 - \zeta_{i,j}^{k,r}\right)\right). \tag{29}$$

Total energy consumption for the ith node and link is calculated by

$$E_{i,\text{total}} = E_{i,\text{node}} + E_{i,\text{link}}. \tag{30}$$

Normalized residual energy is then derived by

$$E_{i,\text{res}} = \left(E_{i,\text{batt}} - E_{i,\text{total}}\right)/E_{i,\text{batt}} \tag{31}$$

where $E_{i,\text{batt}}$ is the initial battery energy of the ith node.

Then, the summation of total trust and normalized residual energy of nodes is given by

$$v = \sum_{i}^{V}\left(NT_i + LT_i + E_{i,\text{res}}\right). \tag{32}$$

The proposed MIP model maximizes v and thereby maximizes the total trust and residual energy of nodes in the network.

The optimization problem is then given by

$$\max \ v \tag{33}$$

subject to:

$$a_i^k \times M \geq x_{i,j}^{k,r} \quad \forall (i,j) \in \boldsymbol{E} \ \forall k \in \boldsymbol{K}, \quad r \in \{1,\ldots,N_r\} \tag{34}$$

$$a_j^k \times M \geq x_{i,j}^{k,r} \quad \forall (i,j) \in \boldsymbol{E} \ \forall k \in \boldsymbol{K}, \quad r \in \{1,\ldots,N_r\} \tag{35}$$

$$\zeta_{i,j}^{k,r} = \begin{cases} 1, & \text{if } m = 0 \wedge n = 1 \text{ and} \\ 0, & \text{o.w.} \end{cases}$$
$$\forall i \in \boldsymbol{V} \quad \forall k \in \boldsymbol{K}, \quad r \in \{1,\ldots,N_r\} \tag{36}$$

$$0 \leq x_{i,j}^{k,r} \leq u_{i,j} \quad \forall k \in \boldsymbol{K} \ \forall (i,j) \in \boldsymbol{E}, \quad r \in \{1,\ldots,N_r\} \tag{37}$$

$$\sum_{\substack{(i,j)\in E \\ (i,j)\notin J}} x_{i,j}^{k,r} - \sum_{\substack{(j,i)\in E \\ (j,i)\notin J}} x_{j,i}^{k,r} = \begin{cases} b^{k,r}, & \text{if } i = s(r) \text{ and} \\ & E_{i,\text{res}} \geq E_{i,\text{th}} \\ -b^{k,r}, & \text{if } i = d(r) \text{ and} \\ & E_{i,\text{res}} \geq E_{i,\text{th}} \\ 0, & \text{if } i = t(r) \text{ or} \\ & E_{i,\text{res}} \leq E_{i,\text{th}} \end{cases}$$
$$\forall i \in \boldsymbol{C} \subseteq \boldsymbol{V}$$
$$\forall k \in \boldsymbol{K}, \quad r \in \{1,\ldots,N_r\} \tag{38}$$

$$\sum_{(i,j)\in E} x_{i,j}^{k,r} - \sum_{(j,i)\in E} x_{j,i}^{k,r} = \begin{cases} b^{k,r}, & \text{if } i = s(r) \\ -b^{k,r}, & \text{if } i = d(r) \\ 0, & \text{if } i = t(r) \end{cases}$$
$$\forall i \in \boldsymbol{D} \subseteq \boldsymbol{V} \quad \forall k \in \boldsymbol{K}, \ r \in \{1,\ldots,N_r\} \tag{39}$$

$$l^{k,r} \times \zeta_{i,j}^{k,r} \leq l_{\text{th}} \quad \forall (i,j) \in \boldsymbol{E} \tag{40}$$

$$x_{i,j}^{k,r} \geq 0 \quad \forall i \in \boldsymbol{V} \ \forall k \in \boldsymbol{K}, \quad r \in \{1,\ldots,N_r\} \tag{41}$$

$$\zeta_{i,j}^{k,r} \in \{0,1\} \quad \forall i \in \boldsymbol{V} \ \forall k \in \boldsymbol{K}. \tag{42}$$

Constraints (35) and (34) ensure that the source node i and the sink node j are active when there is a network flow in the link i,j. This is guaranteed by the big-M parameter where M is a very large number. Constraint (36) switches binary decision variable $\zeta_{i,j}^{k,r}$ to 1 if sensitive data (i.e., $n = 1$) need to be transmitted through an unsecured (e.g., compromised) link (i.e., $m = 0$). Constraint (37) ensures that the rate of flow does not exceed the maximum LC $u_{i,j}$. Constraint (38) enforces flow conservation at all critical nodes and ensures flow only occurs through nonjammed links when the residual energy of critical nodes is greater than the residual energy threshold $E_{i,\text{th}}$. Accordingly, a critical node will not participate in data transfer when its battery is low and while jamming is present, thus minimizing outage risks. Noncritical nodes, however, are still subject to the classical flow conservation constraint given by (39). Constraint (40) ensures that for mission-critical/sensitive data, the latency for the kth flow in route r is less than or equal to a latency threshold. The bounds of the decision variables are specified by (41) and (42).

Since this optimization problem is an MIP, it is considered NP-hard [40]. To solve the MIP and find its exact optimal solution, IBM CPLEX Optimization Studio [41] was used in this work.

IV. Analysis

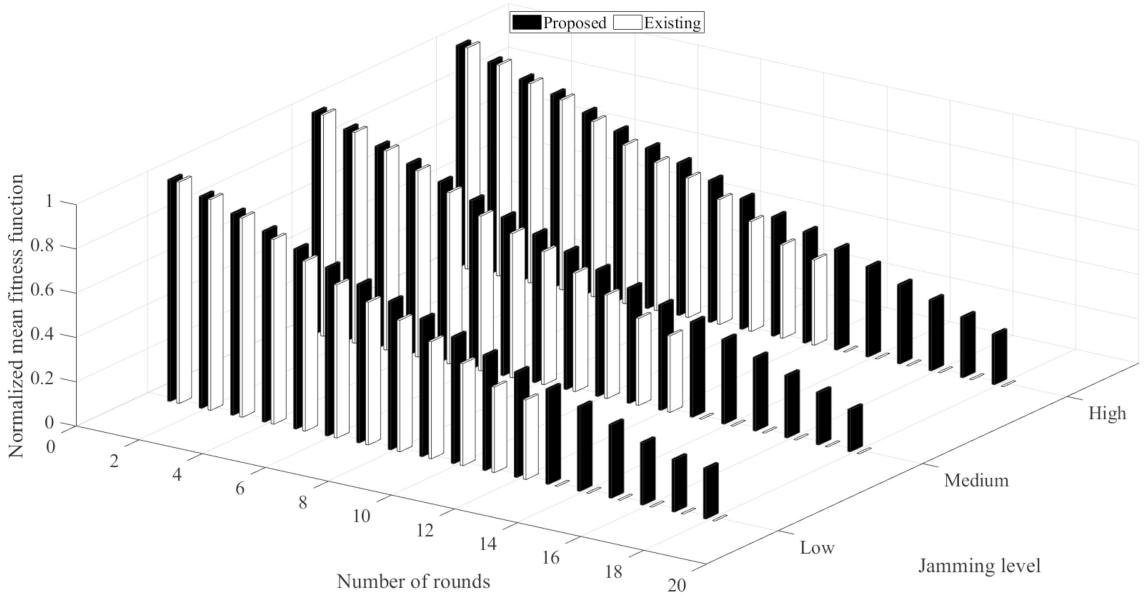
In this section, we discuss the simulation settings and performance evaluation of our proposed solution against existing solutions.

In the context of this performance evaluation, existing solutions are those which do not cache traffic and do not reroute traffic when jamming occurs. Furthermore, existing solutions do not distinguish between sensitive and nonsensitive data and treat all data transmissions with the same level of accessibility. Our proposed solution, however, performs content caching and finds the best route to transmit data during jamming. In addition, it employs a data encryption strategy based on the sensitivity of data. This performance comparison can therefore provide a thorough understanding of how our proposed solution performs against existing solutions.

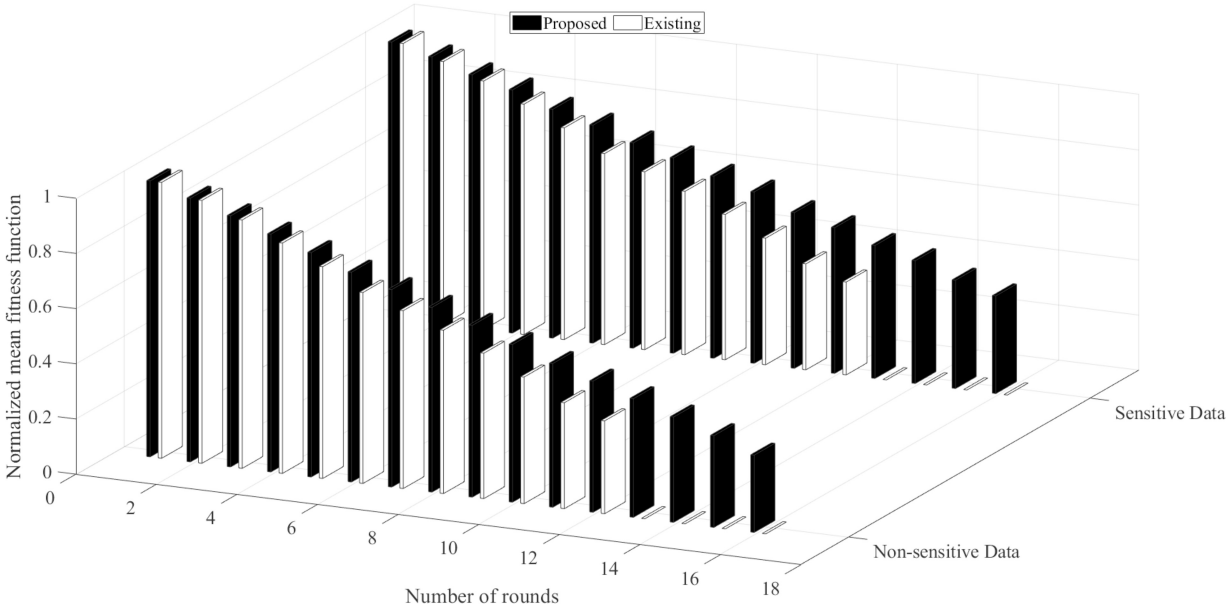
Table I shows the parameter settings required by our proposed solution. We implemented the solution using a network topology containing 19 nodes deployed at different depths within a 1000 m by 1000 m underwater area. Similar to the work in [36], nodes were arranged in ring, star, or tree configurations. To calculate the parametric values required by our solution, we used MATLAB R2019b running on an Intel Xeon E3-1240 3.5-GHz 16-GB RAM PC. The solution to the optimization problem can be achieved under 60 s by using a PC with the aforementioned specifications. Therefore, simulation can be run in real time and does not require extensive execution power.

For analysis, two types of scenarios were considered.

1) *Scenario I (Jamming):* We consider three subscenarios under this scenario, namely, low, medium, and high jamming scenarios. As the name suggests, a lower number of jamming nodes and less frequent jamming has been considered as the low jamming scenario. The same follows for the other two subscenarios. We used periodic jamming for simplicity. However, our solution is not limited to tackling one type of jamming only. Rather, our solution is functional against any type of jamming (e.g., random jamming) as caching occurs regardless of the nature of jamming. For prolonged jamming scenarios, our proposed model will continue to cache data. In



(a)



(b)

Fig. 2. Objective function during two different cases. (a) Jamming scenarios. (b) Sensitive/nonsensitive data transmission scenarios.

these scenarios, the storage capacity of the nodes could be increased for caching data for longer periods. The effects of varying jamming levels (i.e., low, medium, and high) are observed on salient network parameters, such as power consumption, trust, and traffic received, as delivered by both our proposed technique and existing technique. Our proposed technique simultaneously caches content and routes traffic through appropriate links in the presence of jamming. For this scenario, the existing solution used for performance comparison does not cache traffic and does not reroute traffic flow during jamming.

2) *Scenario II (Sensitive Data Transmission):* In this scenario, the optimization model decides whether the content of data transmission requires encryption based on the sensitivity of the data. If data being transmitted is sensitive, our proposed model performs encryption before transmission. If the data being transmitted is not sensitive, our proposed model does not perform any encryption on data. For this scenario, the existing solution used for performance comparison does not distinguish sensitive data from nonsensitive data and encrypts all data transmission by default.

Fig. 2 shows how the objective function [i.e., (33)] that maximizes total trust and residual power of nodes varies over time in the simulation. Fig. 2(a) shows the variation in the objective function over time for Scenario I (i.e., three different

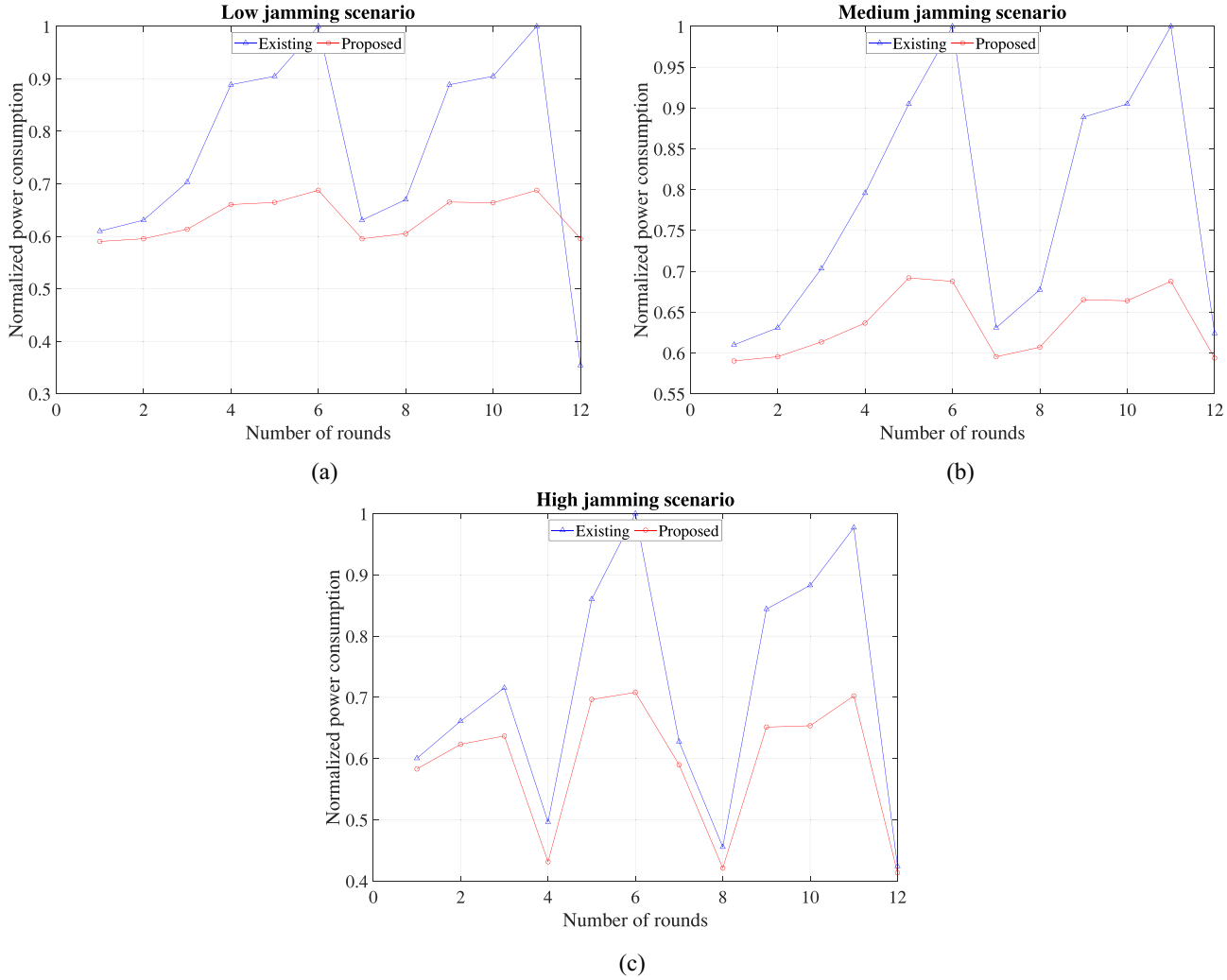


Fig. 3. Normalized power consumption for three scenarios. (a) Low jamming scenario. (b) Medium jamming scenario. (c) High jamming scenario.

jamming scenarios), whereas Fig. 2(b) illustrates the same for Scenario II (i.e., sensitive data transmission).

From Fig. 2(a), it can be observed that the objective function goes to zero for the existing solution a few rounds earlier than that for the proposed solution in all three cases of jamming. This indicates that for the existing solution, the nodes do not have sufficient power to support data transmission. Accordingly, the network lifetime finishes at 12 rounds. In contrast, our proposed solution can offer better network lifetime, where rounds of transmission can continue for up to 18 rounds in all three cases of jamming. Additionally, our proposed solution also yields a higher value for the objective function for every round of transmission during the heavy/high jamming scenario, as compared to medium or low jamming scenarios. This suggests that our proposed technique can better manage total network trust and residual power during highly jammed scenarios.

A similar trend can be observed in Fig. 2(b), where our proposed technique outperforms the existing technique in terms of the objective function. For both nonsensitive and sensitive data transmissions, the existing technique stops data transmission a few rounds earlier than the proposed technique due to insufficient power. During sensitive data transmission, it can be observed that the difference in the objective function between proposed and existing solutions is larger, especially during the later rounds. This indicates that the proposed solution performs better in maximizing trust and residual power when sensitive data is being transmitted.

In order to better understand the solution, we have compared individual parameters, namely, power consumption, trust metric, and traffic serviced for the two scenarios considered.

For Scenario I, we examine the effect of three levels of jamming on power consumption for both proposed and existing solutions. Fig. 3(a)–(c) depicts normalized mean power consumption in the network over time for low, medium, and high levels of jamming, respectively. It can be seen from Fig. 3 that although power consumption slightly increases as more jamming is introduced in the network, it is still lower than the existing technique. It can also be observed that power consumption increases very quickly during jamming scenarios (e.g., indicated by sharp spikes). However, this is only true for the existing technique. Our proposed approach does not experience a massive increase in power consumption in the presence of jamming.

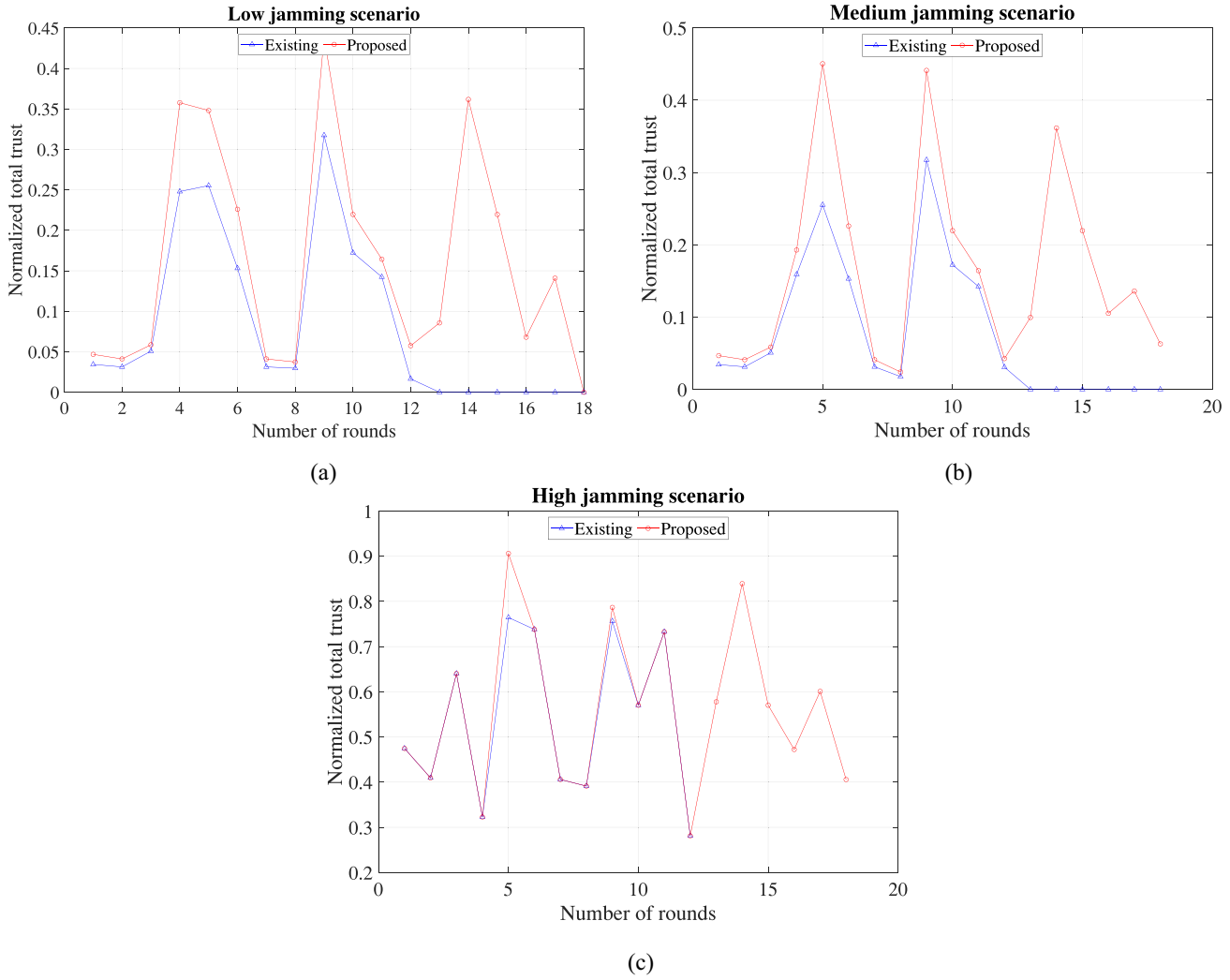


Fig. 4. Normalized trust metric for three scenarios. (a) Low jamming scenario. (b) Medium jamming scenario. (c) High jamming scenario.

Fig. 4 illustrates how the trust component (normalized) of the objective function varies across time in the presence of three jamming levels. It can be clearly observed from the figure that the proposed solution consistently yields a better trust metric as compared to the existing technique. From Fig. 4(c), it can be inferred that during high levels of jamming, our proposed technique yields higher normalized trust values (maximum 0.52) as compared to those during medium and low jamming levels, indicating that the proposed technique performs best when the communication environment is harsh.

Fig. 5 compares the performance of existing and proposed techniques in terms of how well network traffic is serviced by both in the presence of jamming. It can be observed that our proposed solution outperforms the existing solution when heavy jamming occurs [as seen in Fig. 5(c)] by servicing a higher amount of traffic. This is because our proposed solution uses the caching mechanism to store data until the jamming attack is over. It should be noted here that since our proposed technique operates for longer (even after 12 rounds) compared to the existing approach, it can guarantee the delivery of traffic, although sometimes it may be delayed due to extensive jamming.

As mentioned above, we have also investigated the effects of sensitive data transmission on network parameters, such as power consumption, trust, and traffic serviced (i.e., Scenario II). The results of this investigation are presented in Figs. 6–8.

Fig. 6 shows the normalized power consumption for two cases: Fig. 6(a) shows the nonsensitive data scenario and Fig. 6(b) illustrates the sensitive data scenario. For both scenarios, power consumption is higher for the existing solution as compared to our proposed solution. Fig. 7 illustrates the trust metrics for both nonsensitive and sensitive data transmission scenarios and compares the performance of the two solutions. For both scenarios, the area under the curve is greater for our proposed solution as compared to the existing solution. Although there are only a few rounds during the sensitive data scenario that our proposed solution yields a lower trust, the overall trust metric provided is higher because our solution offers a longer network lifetime.

Fig. 8 substantiates the total amount of traffic serviced while transmitting nonsensitive/sensitive data. It can be observed from Fig. 8(a) that the traffic serviced is almost identical

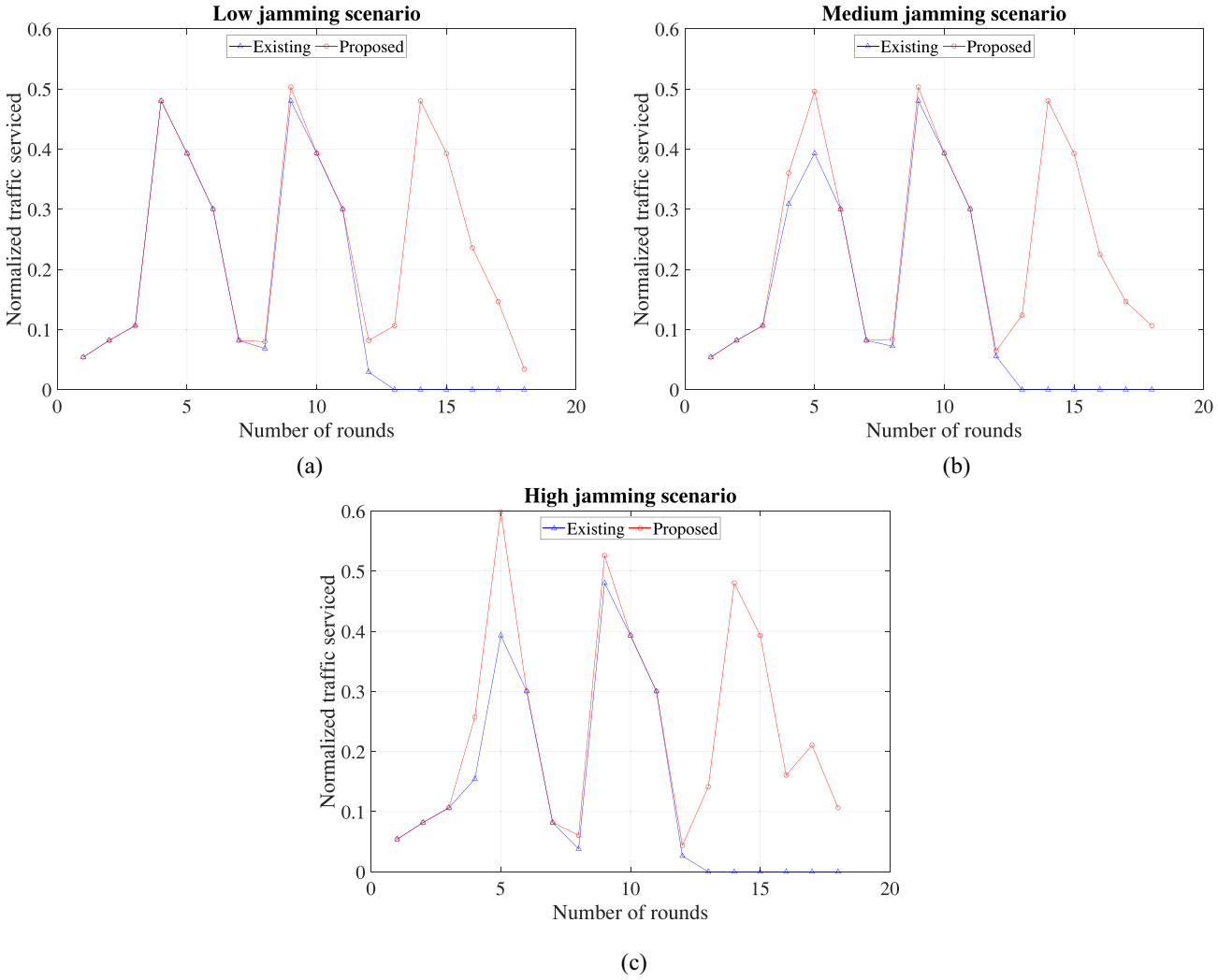


Fig. 5. Normalized traffic serviced for three scenarios. (a) Low jamming scenario. (b) Medium jamming scenario. (c) High jamming scenario.

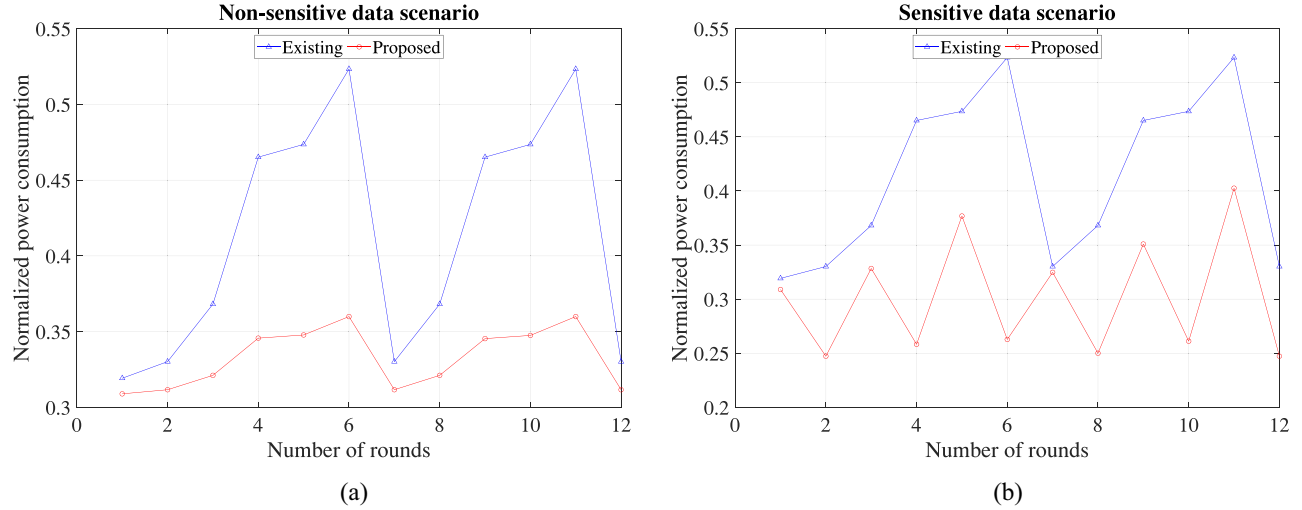


Fig. 6. Normalized power consumption for two scenarios. (a) Non-sensitive scenario. (b) Sensitive scenario.

for both solutions until round 12, after which the network lifetime ends for the existing solution. However, Fig. 8(b) shows that the proposed solution can offer significant improvements in successful traffic delivery when sensitive data is being transmitted. This is because the proposed solution has cache-enabled nodes that can regulate data transmission through secure paths when sensitive data need to be transmitted.

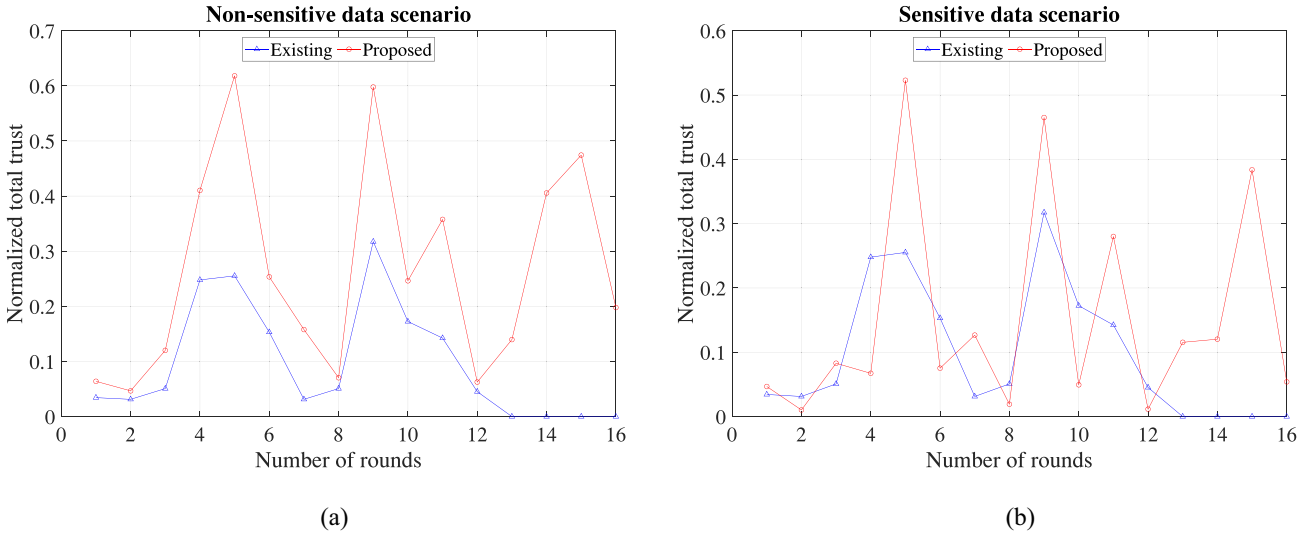


Fig. 7. Normalized trust metric for two scenarios. (a) Non-sensitive scenario. (b) Sensitive scenario.

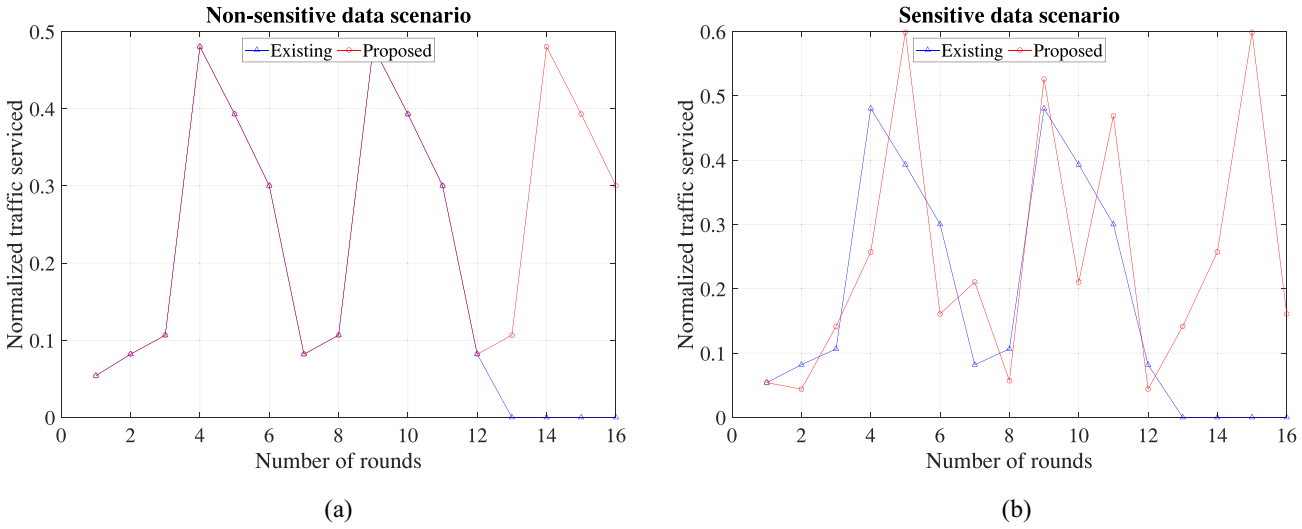


Fig. 8. Normalized traffic serviced for two scenarios. (a) Non-sensitive scenario. (b) Sensitive scenario.

V. Conclusion

UWCNs are becoming increasingly popular in multiple domains, including science, commerce, and the military. However, its widespread adoption also gives way to a number of security challenges. One such prominent security issue is that of jamming, which causes network nodes that are already difficult to recharge/replace to deplete their energy prematurely, resulting in network failure. The other security challenge is to protect the integrity of data transmission through resource-intensive encryption while maintaining a strict energy budget. This work has proposed a solution that addresses both security challenges by leveraging the mechanism of content caching and selectively encrypting sensitive data transmissions. Results indicate that our proposed solution can improve overall network power consumption, trust, and traffic delivery in the presence of jamming as compared to the existing solution. Moreover, our proposed solution yields better results in terms of the aforementioned network parameters when sensitive data is transmitted. This indicates that our proposed solution is a promising mechanism for building energy-efficient and secure UWCNs.

References

[1] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 729–752, 1st Quart., 2019.

[2] J. Heidemann, M. Stojanovic, and M. Zorzi, "Underwater sensor networks: Applications, advances and challenges," *Philosoph. Trans. Roy. Soc. A Math., Phys. Eng. Sci.*, vol. 370, no. 1958, pp. 158–175, 2012.

[3] K. Y. Islam, I. Ahmad, D. Habibi, and A. Waqar, "A survey on energy efficiency in underwater wireless communications," *J. Netw. Comput. Appl.*, vol. 198, Feb. 2022, Art. no. 103295.

[4] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22–28, Feb. 2011.

[5] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, Aug. 2015.

[6] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the development of secure underwater acoustic networks," *IEEE J. Ocean. Eng.*, vol. 42, no. 4, pp. 1075–1087, Oct. 2017.

[7] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, Nov. 2018.
[8] G. Han, Y. He, J. Jiang, N. Wang, M. Guizani, and J. A. Ansere, "A synergetic trust model based on SVM in underwater acoustic sensor networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11239–11247, Nov. 2019.
[9] G. Han, J. Du, C. Lin, H. Wu, and M. Guizani, "An energy-balanced trust cloud migration scheme for underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1636–1649, Mar. 2020.
[10] A. Yazdinejad, R. M. Parizi, G. Srivastava, A. Dehghantanha, and K.-K. R. Choo, "Energy efficient decentralized authentication in Internet of Underwater Things using blockchain," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.
[11] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, and M. N. K. Khattak, "SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 107419–107433, 2020.
[12] O. G. Uyan, A. Akbas, and V. C. Gungor, "A reliable and secure multi-path routing strategy for underwater acoustic sensor networks," *Comput. Netw.*, vol. 212, Jul. 2022, Art. no. 109070.
[13] E. A. Makled and O. A. Dobre, "On the security of full-duplex relay-assisted underwater acoustic network with NOMA," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 6255–6265, Jun. 2022.
[14] L. Xiao, Q. Li, T. Chen, E. Cheng, and H. Dai, "Jamming games in underwater sensor networks with reinforcement learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2015, pp. 1–6.
[15] L. Xiao, D. Jiang, X. Wan, W. Su, and Y. Tang, "Anti-jamming underwater transmission with mobility and learning," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 542–545, 2018.
[16] L. Xiao, D. Jiang, Y. Chen, W. Su, and Y. Tang, "Reinforcement-learning-based relay mobility and power allocation for underwater sensor networks against jamming," *IEEE J. Ocean. Eng.*, vol. 45, no. 3, pp. 1148–1156, Jul. 2020.
[17] A. Signori, F. Chiariotti, F. Campagnaro, and M. Zorzi, "A game-theoretic and experimental analysis of energy-depleting underwater jamming attacks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9793–9804, Oct. 2020.
[18] K. Y. Islam, I. Ahmad, D. Habibi, J. Jin, and M. Waqas, "Lifetime maximization in underwater wireless communication networks," *IEEE Sensors J.*, vol. 22, no. 15, pp. 15549–15560, Aug. 2022.
[19] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.
[20] F. De Souza, R. Souza, G. Brante, M. Pellenz, F. Rosas, and B. Chang, "Code rate optimization for energy efficient delay constrained underwater acoustic communications," in *Proc. OCEANS Genova*, 2015, pp. 1–4.
[21] N. Morozs, W. Gorma, B. T. Henson, L. Shen, P. D. Mitchell, and Y. V. Zakharov, "Channel modeling for underwater acoustic network simulation," *IEEE Access*, vol. 8, pp. 136151–136175, 2020.
[22] A. Stefanov and M. Stojanovic, "Design and performance analysis of underwater acoustic networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2012–2021, Dec. 2011.
[23] R. Francois and G. Garrison, "Sound absorption based on ocean measurements: Part I: Pure water and magnesium sulfate contributions," *J. Acoust. Soc. Am.*, vol. 72, no. 3, pp. 896–907, 1982.
[24] R. Francois and G. Garrison, "Sound absorption based on ocean measurements. Part II: Boric acid contribution and equation for total absorption," *J. Acoust. Soc. Am.*, vol. 72, no. 6, pp. 1879–1890, 1982.
[25] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," in *Proc. 1st ACM Int. Workshop Underwater Netw.*, 2006, pp. 41–47. [Online]. Available: https://doi.org/10.1145/1161039.1161049
[26] H. Esmaiel and D. Jiang, "Review article: Multicarrier communication for underwater acoustic channel," *Int. J. Commun., Netw. Syst. Sci.*, vol. 6, no. 8, p. 361, 2013.
[27] Z. Wei, M. Wang, Z. Chang, and J. Yu, "Comparative simulation of mobile underwater acoustic communication network based on OPNET," in *Proc. Chin. Autom. Congr. (CAC)*, 2020, pp. 7505–7509.
[28] S. Wang, Z. He, K. Niu, P. Chen, and Y. Rong, "New results on joint channel and impulsive noise estimation and tracking in underwater acoustic OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2601–2612, Apr. 2020.
[29] I. F. Enguix, M. S. Egea, A. G. González, and D. A. Serrano, "Underwater acoustic impulsive noise monitoring in port facilities: Case study of the port of cartagena," *Sensors*, vol. 19, no. 21, p. 4672, 2019.
[30] F. Xing, H. Yin, Z. Shen, and V. C. M. Leung, "Joint relay assignment and power allocation for multiuser multirelay networks over underwater wireless optical channels," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9688–9701, Oct. 2020.
[31] J. A. Simpson, B. L. Hughes, and J. F. Muth, "Smart transmitters and receivers for underwater free-space optical communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 5, pp. 964–974, Jun. 2012.
[32] C. M. G. Gussen, P. S. Diniz, M. Campos, W. A. Martins, F. M. Costa, and J. N. Gois, "A survey of underwater wireless communication technologies," *J. Commun. Inf. Syst.*, vol. 31, no. 1, pp. 242–255, 2016.
[33] S. Jaruwatanadilok, "Underwater wireless optical communication channel modeling and performance evaluation using vector radiative transfer theory," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 9, pp. 1620–1627, Dec. 2008.
[34] (Woods Hole Oceanogr. Inst., Falmouth, MA, USA). *Acoustic Communications Group*. Accessed: Aug. 27, 2023. [Online]. Available: https://acomms.whoi.edu/micro-modem/
[35] "LUMA 100: Ultra-efficient wireless optical node," Data Sheet, Hydromea, Renens, Switzerland. Accessed: Aug. 27, 2023. [Online]. Available: https://files.hydromea.com/luma/Hydromea_LUMA_100_datasheet.pdf
[36] K. Y. Islam, I. Ahmad, D. Habibi, M. I. A. Zahed, and J. Kamruzzaman, "Green underwater wireless communications using hybrid optical-acoustic technologies," *IEEE Access*, vol. 9, pp. 85109–85123, 2021.
[37] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, "Research challenges and applications for underwater sensor networking," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2006, pp. 228–235.
[38] M. Doniec, A. Xu, and D. Rus, "Robust real-time underwater digital video streaming using optical communication," in *Proc. IEEE Int. Conf. Robot. Autom.*, 2013, pp. 5117–5124.
[39] S. Han, Y. Noh, U. Lee, and M. Gerla, "Optical-acoustic hybrid network toward real-time video streaming for mobile underwater sensors," *Ad Hoc Netw.*, vol. 83, pp. 1–7, Feb. 2019.
[40] M. Conforti, G. Cornuéjols, and G. Zambelli, *Integer Programming*, vol. 271. Cham, Switzerland: Springer, 2014.
[41] *ILOG CPLEX Optimization Studio User's Manual 12.8*. IBM Technol. Corp., Armonk, NY, USA, USA, 2017.

Kazi Yasin Islam (Member, IEEE) received the Ph.D. degree from Edith Cowan University, Joondalup, WA, Australia, in 2023.

His research interests include underwater wireless communication, green communication, and machine learning.

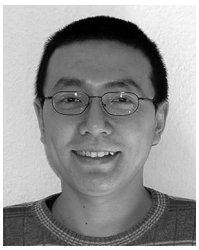
Iftekhar Ahmad (Member, IEEE) received the Ph.D. degree in communication networks from Monash University, Melbourne, VIC, Australia, in 2007.

He is currently an Associate Professor with the School of Engineering, Edith Cowan University, Joondalup, WA, Australia. His research interests include 5G technologies, green communications, QoS in communication networks, software-defined radio, wireless sensor networks, and computational intelligence.

Daryoush Habibi (Senior Member, IEEE) received the B.E. degree (Hons.) in electrical engineering and the Ph.D. degree from the University of Tasmania, Hobart, TAS, Australia, in 1989 and 1994, respectively.

His employment history includes Telstra Research Laboratories, Melbourne, VIC, Australia; Flinders University, Adelaide, SA, Australia; Intelligent Pixels, Inc., Danbury, CT, USA; and Edith Cowan University, Joondalup, WA, Australia, where he is currently a Professor, the Pro Vice-Chancellor, and the Executive Dean of Engineering. His current research interests include engineering design for sustainable development, smart energy systems, environmental monitoring technologies, and reliability and quality of service in communication systems.

Prof. Habibi is a Fellow of Engineers Australia and the Institute of Marine Engineering, Science and Technology.



Yue Rong (Senior Member, IEEE) received the Ph.D. degree (summa cum laude) in electrical engineering from Darmstadt University of Technology, Darmstadt, Germany, in 2005.

He was a Postdoctoral Researcher with the Department of Electrical Engineering, University of California at Riverside, Riverside, CA, USA, from February 2006 to November 2007. Since December 2007, he has been with Curtin University, Bentley, WA, Australia, where he is currently a Professor. His research interests include signal processing for communications, underwater acoustic communications, underwater optical wireless communications, machine learning, speech recognition, and biomedical engineering. He has published over 200 journal and conference papers in these areas.

Prof. Rong is a Senior Area Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING.