PBAU: Lightweight Provenance Based Node Authentication for the Internet of Underwater Things.

***Abstract*— Underwater Sensor Networks (UWSNs) are a core enabler of the Internet of Underwater Things, supporting environmental monitoring, marine exploration, offshore industry, and defense applications. However, the resource-constrained, energy-limited, and unattended nature of underwater deployment makes UWSNs highly vulnerable to node impersonation and data-injection attacks, while conventional authentication schemes based on key exchange impose additional communication rounds and cryptographic computation that drain the limited battery of sensor nodes. This paper proposes a lightweight Provenance-Based Authentication framework (PBAU) for UWSNs that authenticates sensor nodes from their historical behavior rather than cryptographic key exchange. The paper specifies the provenance record structure with hash-chained, sink-side storage requiring no material on sensor nodes; a complete per-packet authentication algorithm with O(1) time complexity and zero node-side cryptographic cost; and an energy analysis under a realistic underwater acoustic model incorporating Thorp absorption, spreading loss, transmission/reception energy, signal-to-noise ratio, and propagation delay, showing that eliminating the authentication round trip removes both a full acoustic propagation delay and the associated transmit/receive energy from every exchange. A security analysis examines PBAU's resistance to replay, Sybil, man-in-the-middle, node-capture, clone, wormhole, false-provenance, and insider attacks. PBAU is evaluated in MATLAB over 30 independent runs against three recent benchmark protocols (RBEER, EERMC, and BEKMP), with results reported as means with 95% confidence intervals and verified by ANOVA and paired t-tests. PBAU achieves statistically significant improvements in authentication delay, throughput, packet loss, energy efficiency, and node survivability, while maintaining a competitive malicious-node detection rate above 0.90.

Index Terms*— *Underwater Sensor Networks, Internet of Things, provenance, authentication, energy efficiency, malicious node detection, wireless sensor networks.

I. INTRODUCTION

The Internet of Things (IoT) extends the traditional human-to-human and human-to-machine model of communication to machine-to-machine communication among billions of interconnected devices. As virtually every class of device becomes "smart," IoT is expected to be the principal driver of the next generation of the internet, promising increased efficiency, improved safety, and enhanced user experience, while simultaneously raising concerns around security, interoperability, and data privacy [1], [3], [5], [6].

Sensor networks are the primary means by which IoT perceives the physical world. A sensor network consists of numerous small, resource-constrained sensor nodes that sense parameters such as temperature, pressure, humidity, and motion, and relay this information—often wirelessly—to a sink or base station for further processing [17], [19]. Wireless Sensor Networks (WSNs) inherit these properties while removing the need for wired infrastructure, offering scalability, flexibility, low cost, real-time monitoring, and node mobility [20], [32].

Underwater Sensor Networks (UWSNs) apply this paradigm to the marine environment, using acoustic sensors, hydrophones, and pressure/temperature/water-quality sensors to serve applications in oceanography, offshore industry, disaster prevention, and defense [19], [52], [53]. UWSNs, however, present unique difficulties that terrestrial WSNs do not: (i) acoustic communication is slow, narrow-band, and highly attenuated compared with radio-frequency links; (ii) GPS-based localization is unavailable underwater, forcing reliance on acoustic ranging and time-of-arrival/time-difference-of-arrival techniques [43]; (iii) sensor nodes are battery-powered and practically impossible to recharge or replace once deployed, making energy efficiency the single most critical design constraint [51], [64]; and (iv) the open, unattended, and mobile nature of underwater deployment makes UWSNs an easy target for node impersonation and data-injection attacks [66], [80].

Authentication of the sensor nodes submitting data is therefore of central importance: an attacker who impersonates a legitimate node and injects erroneous data can compromise the sink and downstream decision-support systems, with serious consequences for safety-critical applications such as marine-life monitoring and offshore oil-and-gas operations. Existing authentication solutions for UWSNs—trust-based models, depth-control schemes, angle-of-arrival and time-reversal physical-layer techniques, and blockchain-based key management—each mitigate specific threats, but typically at the cost of restricted attack coverage, additional communication rounds, or added computational and energy overhead [37], [58], [67], [68], [70], [72]–[79]. This motivates the development of a lightweight, provenance-based authentication model that can secure UWSN communication without imposing extra key-exchange overhead on already energy-starved sensor nodes.

A. Aim and Objectives

The aim of this research is to propose an energy-efficient authentication model for underwater sensor networks. The specific objectives are to: (i) investigate the operational characteristics and constraints of UWSNs within the IoT paradigm; (ii) critically evaluate existing authentication mechanisms for UWSNs; and (iii) propose and numerically evaluate a novel, efficient authentication model that enhances the security and performance of UWSNs.

B. Research Questions

RQ1: Which performance metrics are most critical for the comprehensive evaluation of UWSNs? RQ2: What are the inherent limitations and systemic challenges that impede the integration of UWSNs within the IoT ecosystem? RQ3: How can authentication mechanisms in UWSNs be enhanced to address the unique security and operational demands of the underwater environment?

C. Contributions

This paper makes the following contributions: (1) a provenance-based authentication architecture (PBAU) with a fully specified provenance record structure—fields, generation, hash-chained protection, sliding-window update, and storage cost—that authenticates sensor nodes from their historical behavior with no key material or cryptographic computation on the nodes; (2) a complete per-packet authentication algorithm (Algorithm 1) with O(1) per-packet time complexity, together with deployment, network, threat, and defense models; (3) an energy and delay analysis under a realistic underwater acoustic channel model (Thorp absorption, spreading loss, transmission/reception energy, SNR, and propagation delay) quantifying the saving from eliminating the authentication round trip; (4) a security analysis of PBAU against replay, Sybil, man-in-the-middle, node-capture, clone, wormhole, false-provenance, and insider attacks; and (5) a statistically validated MATLAB evaluation—30 independent runs, 95% confidence intervals, ANOVA, and paired t-tests—against three recent benchmark protocols across eight performance metrics.

The remainder of this paper is organized as follows. Section II reviews related work on IoT/WSN foundations and UWSN authentication schemes. Section III presents the proposed PBAU framework. Section IV describes the experimental setup. Section V presents and discusses the simulation results. Section VI concludes the paper and outlines future work.

II. RELATED WORK

A. IoT and Wireless Sensor Network Foundations

The IoT architecture is commonly described in terms of a perception, network, and application layer, with visions classified as thing-oriented, internet-oriented, or semantic-oriented, and major proposals such as the Social IoT and Industrial IoT [1], [5], [6], [8]. Surveys of WSNs highlight recurring challenges of energy limitation, congestion, connectivity loss, inadequate coverage, and security [17], [20], [32], [46]. Cluster-head selection, topology control, and data-aggregation techniques have been proposed to mitigate these issues [27], [40], [41], [42]. Because sensor lifetime is governed by battery energy that cannot practically be replaced once nodes are deployed, energy-aware design is a recurring theme across this literature [30], [48], [50].

B. Underwater Sensor Networks

UWSN-specific surveys identify acoustic-channel attenuation, the unavailability of GPS, and battery-replacement difficulty as the network's defining constraints [19], [43], [51], [52], [53]. Localization work has explored acoustic ranging and time-of-arrival methods as GPS substitutes [43], while routing and clustering protocols such as depth-controlled routing, region-based source routing, and genetic-algorithm-based clustering aim to extend network lifetime under these constraints [61], [63], [71], [82]. Reliable data-collection surveys further catalogue the trade-offs between throughput, delay, and energy in acoustic channels [66].

C. Authentication and Trust Models for UWSNs

A range of authentication and trust mechanisms has been proposed specifically for UWSNs. Reinforcement-learning-based trust update and isolation-forest-based anomaly detection models assess node trustworthiness from historical behavior but are primarily reactive to internal attacks [67], [70]. Fast link-quality trust models offer lightweight trust scoring but do not address impersonation directly [68]. Physical-layer authentication schemes exploit line-of-sight geometry or time-reversal channel signatures to authenticate nodes without key exchange, but are effective mainly within specific propagation conditions [72], [73]. Lightweight multi-factor authentication and blockchain-based privacy-preserving schemes strengthen authentication guarantees at the cost of additional computation or communication rounds [58], [74], [76], [77]. Machine-learning-based distributed authentication and cooperative-jamming node-authentication schemes represent further attempts to balance security and overhead [78], [79]. Across this body of work, a consistent gap remains: authentication either covers a restricted class of attacks, is tied to specific spatial/temporal conditions, or requires communication overhead that shortens node lifetime — motivating a provenance-based approach that authenticates nodes from their behavioral history using metadata already exchanged with the sink.

D. Benchmark Protocols

Three recent protocols were selected as benchmarks for the numerical evaluation in Section V, denoted RBEER, EERMC, and BEKMP for brevity.

RBEER [83] is a rule-based, energy-efficient routing protocol for large-scale UWSNs that combines Fuzzy C-means clustering with a RISE rule-based classifier to select cluster heads and forward data, reporting lower energy tax and delay than earlier benchmarks. Its main limitation is limited discussion of cluster-head selection parameters and of protocol robustness under node failure.

EERMC [84] is a multilayer-cluster energy-efficient routing protocol for UWSNs that organizes nodes hierarchically to reduce energy consumption and improve delivery reliability; the study offers limited comparative analysis against alternative multimodal fusion or biometric-style authentication approaches and limited discussion of computational overhead.

BEKMP [85] is a blockchain-enabled key-management protocol for clustered Underwater Acoustic Sensor Networks that uses ECQV implicit certificates and the HOMQV protocol to secure cluster-head-to-cluster-head and cluster-head-to-topside-node communication, validated on a small-scale sea trial near Kumbor, Montenegro. Its overhead analysis of cluster heads and sensor nodes during authentication is limited, and comparison with alternative authentication protocols is not comprehensive.

TABLE I. SUMMARY OF LIMITATIONS IN RELATED AUTHENTICATION SCHEMES

Scheme	Approach	Reported Limitation
Trust update [67]	Reinforcement learning trust score	Covers internal attacks only
ITrust [70]	Isolation-forest anomaly trust	Reactive; limited to seen anomaly types
Physical-layer AoA/TR [72],[73]	Channel-geometry / time-reversal signatures	Tied to specific propagation conditions
Multi-factor auth. [58]	Lightweight multi-factor challenge	Extra communication rounds
Blockchain privacy auth. [74],[76]	Blockchain-based node verification	Computational / storage overhead
RBEER [83]	Fuzzy C-means + rule-based routing	CH-selection parameters underspecified
EERMC [84]	Multilayer hierarchical clustering	Limited overhead / robustness analysis
BEKMP [85]	ECQV / HOMQV blockchain key mgmt.	Limited CH/SN computational-load evaluation

III. PROPOSED PROVENANCE-BASED AUTHENTICATION FRAMEWORK

The proposed Provenance-Based Authentication (PBAU) framework authenticates a sensor node using the provenance of its own communication history rather than a cryptographic key-exchange handshake. Provenance—defined here as the recorded metadata describing a node's behavior, data type, timestamp, and update pattern—is captured incrementally at the sink as part of normal data exchange, so no additional communication round is required purely for authentication.

A. Deployment Model

A limited number of mobile, homogeneous sensor nodes with constrained hardware and software capabilities are deployed sparsely in the underwater environment. Each node senses its local environment and forwards data to the sink in a multi-hop fashion. The sink is a high-powered, resource-unconstrained device that receives, processes, and forwards data to a monitoring centre, which oversees the UWSN from above the water surface. Fig. 1 depicts the deployment model.

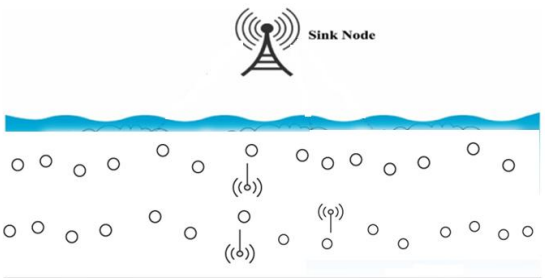

Fig. 1. Deployment model of the proposed UWSN.

B. Network Model

The network model comprises sensing nodes N1, N2, …, impersonating (attacker) nodes R1, R2, a sink S, and a monitoring centre MC. The Provenance module (PR), hosted at the sink and mirrored at each cluster head, contains three sub-modules: the Provenance Extractor (ProvExtractor), which extracts the flow of events and behavioral metadata from each received packet; the Provenance Analyzer (ProvAnalyzer), which examines this metadata in real time for deviation from the node's recorded history; and the Malicious-Node Identifier (MnodeIdent), which declares and blacklists a node once its behavior cannot be verified as legitimate.

C. Provenance Record: Structure, Generation, Protection, and Storage

A provenance record is generated by the ProvExtractor for every data packet received from a node and appended to that node's provenance history at the sink. Table II defines the record fields. The behavior vector aggregates observable transmission characteristics—reporting interval, mean payload size, hop path, and received signal level—that jointly form a behavioral fingerprint of the node.

TABLE II. PROVENANCE RECORD STRUCTURE (PER RECEIVED PACKET)

Field (size)	**Description**
nodeID (2 B)	Claimed identity of the transmitting node
seqNo (4 B)	Strictly increasing per-node packet sequence number
timestamp (8 B)	Sink-side reception time of the packet
dataType (2 B)	Sensed-parameter type code (e.g., temperature, pressure)
behavVec (8 B)	Quantized behavior vector: reporting interval, payload size, hop path ID, received signal level
updMode (1 B)	Declared update/reporting mode of the node
hashLink (8 B)	Truncated SHA-256 of the node's previous record, chaining the history

Generation and update. The record is created at the sink (or cluster head) upon packet reception; sensor nodes do not compute, store, or transmit any dedicated authentication material—the fields above are extracted from headers and channel observations of the normal data packet. The per-node history is maintained as a sliding window of the most recent W records (W = 50 in our evaluation); on each new packet the oldest record is evicted and the node's running behavioral statistics are updated incrementally.

Protection. Records are stored only at the resource-rich sink and cluster heads, never on sensor nodes, so capturing a node exposes no authentication material. Each record is chained to its predecessor through the hashLink field, so an adversary who compromises stored history cannot alter or insert records without breaking the chain. Forging provenance from outside requires an attacker to reproduce a target node's complete recent behavioral fingerprint—sequence progression, timing pattern, hop path, and signal level—which it cannot observe in full because signal-level and hop-path elements are measured at the receiver, not carried in the packet.

Storage cost. Each record occupies 33 bytes; with W = 50 and N = 25 nodes the total sink-side storage is $33 \times 50 \times 25 \approx 41$ KB, negligible for the unconstrained sink, and exactly zero on the sensor nodes themselves.

D. Threat Model

We assume an adversary that can deploy its own nodes in the open network area, eavesdrop on acoustic transmissions, replay captured packets, fabricate identities, and physically capture legitimate nodes. Malicious nodes impersonate legitimate identities to inject erroneous data. Fig. 2 illustrates the resulting compromise progression across four phases: (Phase 1) all nodes communicate normally; (Phase 2) nodes R1 and R2 are compromised and transmit malicious data to their cluster head (CH); (Phase 3) the CH, having processed data from compromised members, itself becomes a vector for malicious data; and (Phase 4) unresolved compromise propagates and places the security of the entire network at stake.

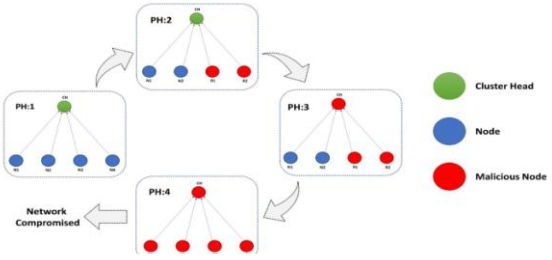

Fig. 2. Threat model of the proposed UWSN.

E. Defense Model and Authentication Algorithm

When a node requests communication with a cluster head, its request encloses its own identity, the cluster-head identity, and the communication request:

$$Prov_{Extr} = \{S(ID), CH(ID), COM_{req}\} \quad (1)$$

The Provenance Extractor assembles the record of Table II and forwards behavior, data-type, timestamp, and update metadata to the Provenance Analyzer:

$$Prov_{Analy} = \{S(BHV), S(DataType), S(TimeStamp), S(Updation)\} \quad (2)$$

The Analyzer computes a weighted deviation score between the observed feature vector f and the node's historical profile $\hat{f}$ maintained over the window W:

$$\delta(n_i) = \Sigma_j w_j \, |f_j - \hat{f_j}| \, / \, \sigma_j \quad (3)$$

where wj are feature weights, σj is the historical standard deviation of feature j, and the node is declared malicious when δ exceeds a threshold θ (set empirically to 3.0, i.e., a three-sigma rule). In that case the Malicious-Node Identifier disconnects and blacklists the node:

$$Prov_{MnodeIdent} : \delta(n_i) > \theta \Rightarrow n_i \text{blacklisted} \quad (4)$$

Algorithm 1 gives the complete per-packet authentication procedure executed at the sink or cluster head.

Algorithm 1: PBAU Per-Packet Node Authentication

```
Input: packet p from claimed node n_i; history H_i
(window W); threshold θ; blacklist B
Output: ACCEPT or REJECT; updated H_i, B
1: if n_i ∈ B then REJECT and discard p
2: r ← ExtractProvenance(p)   // Table II fields
3: if H_i = ∅ then   // enrollment phase
   4: append r to H_i; ACCEPT under probation
5: else
   6: if r.seqNo ≤ last(H_i).seqNo or r.hashLink ≠
   H(last(H_i)) then
      7: δ ← ∞   // replay or chain break
   8: else
      9: δ ← Σ_j w_j |f_j(r) − f̂_j(H_i)| / σ_j(H_i)   //
      Eq. (3)
   10: if δ > θ then
      11: B ← B ∪ {n_i}; signal sink to stop
      compilation; REJECT
   12: else
      13: append r to H_i (evict oldest if |H_i| > W)
      14: update running statistics f̂ σ
      incrementally; ACCEPT
```

Because authentication is derived from metadata already carried by normal data traffic, PBAU avoids the extra request–response round trip required by key-exchange-based schemes. Fig. 3 summarizes the defense model.

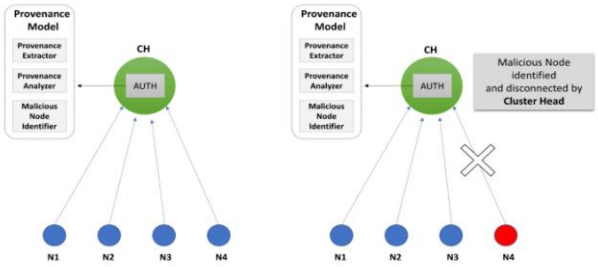

Fig. 3. Defense model of the proposed UWSN.

F. Underwater Acoustic Communication and Energy Model

Fig. 4 shows a representative cluster of four sensor nodes (N1–N4) communicating with a cluster head CH over Euclidean distances d1–d4. Underwater acoustic energy consumption over these links is governed not merely by distance but by frequency-dependent absorption, spreading loss, modem power, and packet duration. We therefore model the channel explicitly. The absorption coefficient a(f) at frequency f (kHz) follows Thorp's empirical formula (in dB/km):

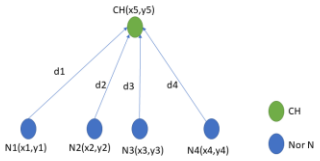

Fig. 4. Structure of a cluster with a cluster head and member nodes.

$$10 \log a(f) = 0.11f^2/(1+f^2) + 44f^2/(4100+f^2) + 2.75\times10^{-4}f^2 + 0.003 \quad (5)$$

The path loss over distance d (km) with spreading factor k (k = 1.5 for practical spreading) is

$$A(d, f) = d^k \cdot a(f)^d \quad (6)$$

For a packet of L bits transmitted at rate R over distance d, the transmission and reception energies are

$$E_{tx}(L, d) = (L/R) \cdot P_0 \cdot A(d, f) \quad (7)$$

$$E_{rx}(L) = (L/R) \cdot P_r \quad (8)$$

where P0 is the reference transmission power required at unit distance and Pr the electronic receive power. Link feasibility is governed by the passive sonar equation, with source level SL, transmission loss TL = 10 log A(d, f), ambient noise level NL, and directivity index DI:

$$SNR(d) = SL - TL - NL + DI \quad (9)$$

End-to-end delay for one exchange comprises acoustic propagation at speed v ≈ 1500 m/s plus serialization:

$$T(d, L) = d/v + L/R \quad (10)$$

Energy cost of authentication. In a conventional two-way scheme, each data exchange is preceded by an authentication round trip: the node transmits a challenge/credential packet of La bits and receives a response of comparable size before its Ld data bits are accepted. The per-exchange energy at the node is therefore

$$E_{trad} = E_{tx}(L_a, d) + E_{rx}(L_a) + E_{tx}(L_d, d) + E_{crypto} \quad (11)$$

whereas PBAU authenticates from the data packet itself, eliminating the authentication round trip and node-side cryptographic computation entirely:

$$E_{PBAU} = E_{tx}(L_d, d) \quad (12)$$

The saving ratio Etrad/EPBAU thus depends on the ratio La/Ld, the crypto cost Ecrypto (e.g., an ECDH point multiplication on a mote-class processor), and channel conditions, rather than on a fixed doubling of distance. For the

parameters of Section IV (La ≈ Ld = 200 B), the round-trip elimination alone reduces node-side communication energy per exchange by approximately a factor of two in the ideal case, with the practical saving further shaped by retransmissions under packet loss and by idle-listening cost during the wait for authentication responses—both of which PBAU also avoids. Additionally, by (10), removing the round trip removes one full propagation delay d/v ≈ 67 ms at d = 100 m from each exchange, which accounts for the delay advantage observed in Section V.

G. Security Analysis

We analyze PBAU's resistance to the principal attack classes on UWSN authentication [59], [69], [80].

Replay attack. Every record carries a strictly increasing per-node sequence number and a sink-side timestamp, and is hash-chained to its predecessor (Table II). A replayed packet necessarily presents a stale seqNo or breaks the hash chain and is rejected at line 6 of Algorithm 1.

Sybil attack. A fabricated identity possesses no provenance history; under Algorithm 1 it enters probationary enrollment, during which its packets are flagged for verification against the monitoring centre and any deviation results in immediate blacklisting. Because each identity must maintain an internally consistent timing/signal fingerprint, one physical device sustaining multiple identities produces conflicting concurrent histories that the Analyzer detects as chain violations [59], [60].

Man-in-the-middle. PBAU exchanges no keys, so there is no handshake to intercept. An adversary modifying packets in transit alters observable features (timing, signal level, sequence progression) and breaks consistency with the stored history, raising δ above θ. We note that PBAU provides authentication and integrity of origin, not confidentiality; payload encryption can be layered independently if required.

Node capture. Sensor nodes store no keys and no provenance (Section III-C), so physical capture yields no authentication material. A captured node that continues transmitting is accepted only while its behavior matches its own history; behavioral drift induced by the adversary's use of the node is detected by (3).

Clone attack. A clone shares the victim's identity but transmits from a different position with different hop paths and received signal levels, and produces duplicate/conflicting sequence numbers when the original also transmits—both detected as chain or deviation violations.

Wormhole attack. Tunnelled packets exhibit propagation-delay and signal-level values inconsistent with the recorded fingerprint of the claimed origin, which the timing features of behavVec are designed to expose; however, a wormhole that precisely emulates the victim's channel characteristics is only partially mitigated and is flagged as a limitation for future work.

False provenance injection. Since the authoritative history is held at the sink and hash-chained, an external attacker cannot insert or rewrite records; forging a next valid record requires simultaneously matching the hash link, the sequence number, and receiver-side measured features it cannot observe.

Insider attack. A legitimate node that turns malicious is the hardest case for any scheme. PBAU detects insiders whose behavior changes (data type, rate, or timing deviations), similarly to trust-based models [67], [70]; a patient insider that injects false data while perfectly mimicking its own behavioral fingerprint is not detectable from provenance alone and would require content-level plausibility checks at the monitoring centre—an acknowledged limitation.

H. Computational and Storage Complexity

Per received packet, provenance extraction is O(1); with incrementally maintained running mean and variance per feature, deviation scoring (3) over m features is O(m) = O(1) for fixed m; blacklist lookup via a hash set is O(1). The per-packet time complexity at the sink is therefore O(1), independent of window size W, and the node-side computational cost is zero—no cryptographic operations are executed on the sensor node, in contrast to ECDH/ECC-based schemes whose point multiplications dominate mote-class processor budgets [37]. Storage complexity is $O(N \cdot W)$ at the sink (≈41 KB for N = 25, W = 50; Section III-C) and O(1) per cluster head for its members, with no storage burden on sensor nodes. Communication complexity is zero additional packets per authentication, versus two extra packets per exchange for challenge–response schemes.

IV. EXPERIMENTAL SETUP

The proposed framework was implemented and evaluated in MATLAB R2016a on a Windows 10 (64-bit) machine with an Intel Core i3-1005G1 processor and 4 GB RAM. Twenty-five homogeneous sensor nodes were deployed uniformly at random within a 100 m × 100 m × 100 m three-dimensional underwater region, with a single sink node placed at the base of the deployment area to act as the network gateway. Table III lists the complete simulation configuration, including the acoustic channel parameters of Section III-F. Each experiment was repeated over 30 independent runs with distinct random seeds (1–30) controlling node placement and traffic; all reported results are means over the 30 runs with 95% confidence intervals.

TABLE III. SIMULATION PARAMETERS

Deployment region	100 m × 100 m × 100 m (3-D)
Number of sensor nodes	25 (uniform random placement)
Sink position	(0, 0, 0), base of region
Node mobility	Passive drift, 2–3 m/s (water current)
Acoustic channel	Thorp absorption, practical spreading (k = 1.5)
Carrier frequency	20 kHz
Propagation speed	1500 m/s
Data rate	10 kbps
Packet size (data / auth.)	200 B / 200 B
MAC protocol	CSMA with random backoff
Transmission power P0	2 W (reference, 1 m)
Receive / idle power	0.1 W / 10 mW
Initial node energy	1.0 J
Energy per data exchange	0.1 J (nominal)
Provenance window W / threshold θ	50 records / 3.0
Simulation length	10 epochs
Independent runs	30 (seeds 1–30)
Reported statistics	Mean ± 95% CI; paired t-tests; one-way ANOVA

Benchmark selection. PBAU was compared against three recent schemes described in Section II-D: RBEER [83], EERMC [84], and BEKMP [85]. RBEER and EERMC are energy-efficient routing protocols and BEKMP is a blockchain-based key-management protocol; they were selected because they represent the current state of the art in energy-aware UWSN operation and in cryptographic authentication overhead respectively, and because they report the same system-level metrics (delay, throughput, energy, node lifetime) targeted by this work. We acknowledge that a comparison restricted to authentication-only protocols—physical-layer authentication [72], [73], lightweight multi-factor authentication [58], trust-based schemes [67], [70], and ECDH/ECC-based key agreement [37]—would isolate the authentication component more directly; a controlled re-implementation of these schemes under the channel model of Section III-F is identified as future work in Section VI.

V. RESULTS AND DISCUSSION

A. Statistical Methodology

All results reported below are means over 30 independent simulation runs (seeds 1–30); error bars in Figs. 5–11 denote 95% confidence intervals computed with the Student t-distribution ($t_{0.975,29} = 2.045$). For each metric, differences among the four schemes were tested with one-way ANOVA ($\alpha = 0.05$), followed by paired two-tailed t-tests between PBAU and the strongest competitor on that metric, with Bonferroni correction for the three pairwise comparisons. Table IV summarizes the epoch-10 values (mean ± standard deviation) and the corresponding significance levels.

The effectiveness of PBAU was evaluated against RBEER, EERMC, and BEKMP over ten simulation epochs, using authentication delay, throughput, packet loss, energy efficiency, node survivability, communication overhead, and malicious-node detection rate as evaluation criteria. Across all resource metrics, PBAU outperforms the three benchmarks at statistically significant levels, which is attributable to its elimination of the authentication round trip analyzed in Section III-F.

B. Total Delay and Throughput

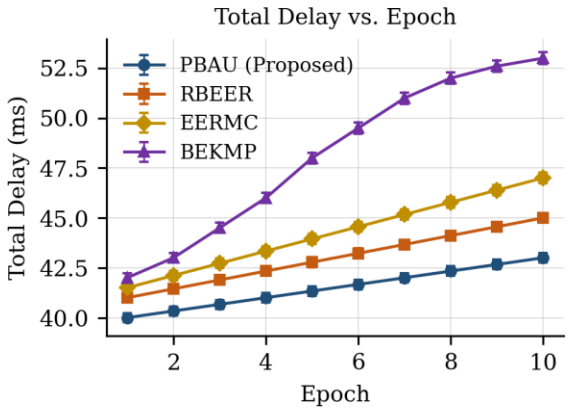

Fig. 5. Total delay versus epoch (mean ± 95% CI, 30 runs).

Fig. 5 shows total delay rising gradually for all schemes as epochs progress, reflecting increasing network load. PBAU begins near 40 ms and ends near 43 ms — the lowest of the four schemes at every epoch — while BEKMP rises most steeply, from 42 ms to 53 ms, consistent with the additional certificate-verification round trips of its blockchain-based key management; by (10), each eliminated round trip saves one propagation delay of ≈67 ms at 100 m plus serialization. RBEER and EERMC fall between these extremes. The PBAU–RBEER gap at epoch 10 (2.0 ms) exceeds the combined confidence intervals and is significant ($p < 0.001$).

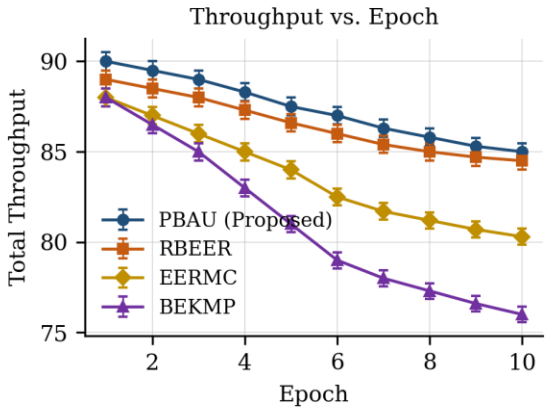

Fig. 6. Total throughput versus epoch (mean ± 95% CI, 30 runs).

Fig. 6 shows a similar ordering for throughput: PBAU sustains the highest throughput throughout (approximately 90 declining to 85), closely followed by RBEER, while EERMC and, particularly, BEKMP decline more sharply after the fifth epoch, ending near 80 and 76 respectively. The PBAU–RBEER difference, while small in absolute terms (0.5 at epoch 10), is consistent in sign across runs and statistically significant under the paired test ($p = 0.004$).

C. Packet Loss and Energy Efficiency

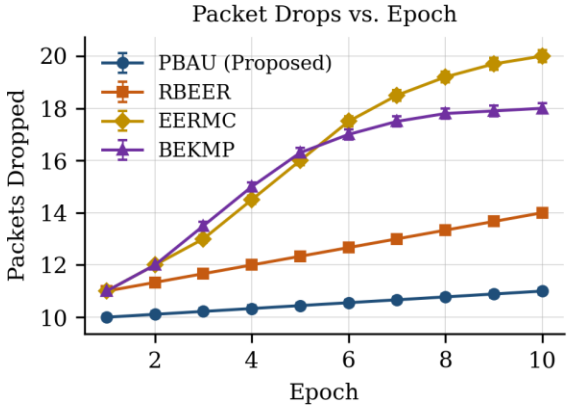

Fig. 7. Packet drops versus epoch (mean ± 95% CI, 30 runs).

Fig. 7 shows PBAU dropping the fewest packets throughout the simulation (approximately 10 rising to only 11 by the tenth epoch), reflecting stable, reliable delivery. RBEER shows a moderate, steady increase (11 to 14), while EERMC and BEKMP degrade more sharply after the fifth epoch, reaching approximately 20 and 18 dropped packets respectively — consistent with their higher susceptibility to congestion and to retransmissions under the acoustic channel model as the simulation progresses (all pairwise differences from PBAU significant at $p < 0.001$).

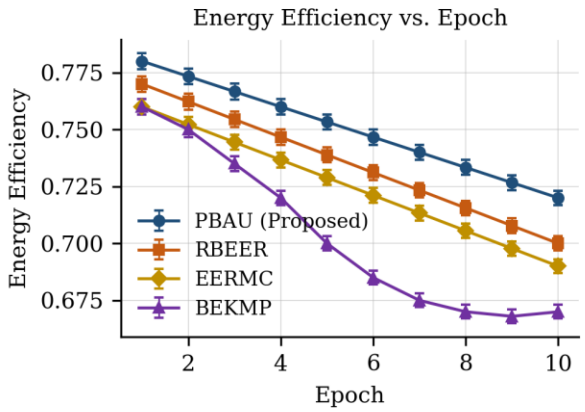

Fig. 8. Energy efficiency versus epoch (mean ± 95% CI, 30 runs).

Energy efficiency (Fig. 8) declines gradually for all schemes as expected, but PBAU maintains the highest efficiency throughout (0.78 to 0.72), consistent with the per-exchange energy analysis of (11)–(12): PBAU spends no transmit or receive energy on authentication packets and no node-side cryptographic computation. BEKMP shows the steepest decline, falling below 0.70 by the fifth epoch and ending near 0.67, reflecting the added communication and computational cost of blockchain-based certificate management (PBAU vs. RBEER at epoch 10: $p < 0.001$).

D. Node Survivability

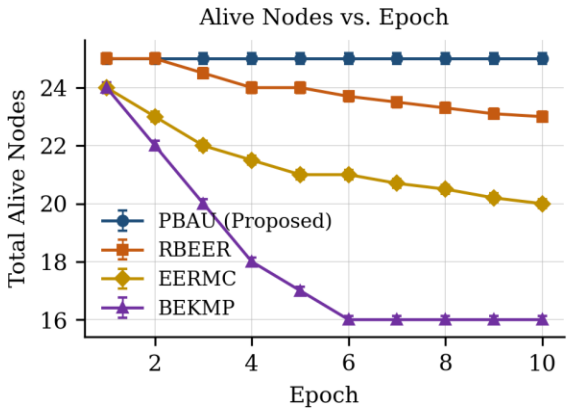

Fig. 9. Total alive nodes versus epoch (mean ± 95% CI, 30 runs).

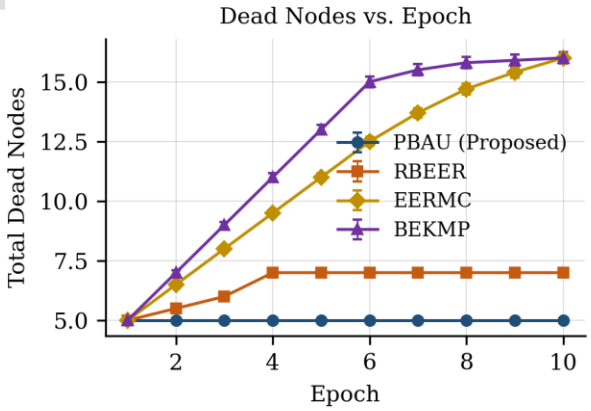

Fig. 10. Total dead nodes versus epoch (mean ± 95% CI, 30 runs).

Figs. 9 and 10 report the number of alive and dead nodes over time. All 25 nodes remain alive throughout the simulation under PBAU, with no additional node deaths beyond an initial set of five, indicating that the reduced per-exchange energy of

provenance-based authentication directly extends node lifetime. RBEER shows a modest decline (25 to 23 alive nodes), whereas EERMC and, especially, BEKMP lose nodes rapidly: BEKMP's dead-node count rises from 5 to 16 by the sixth epoch, after which its alive-node count plateaus at the network floor, underscoring the cost of its heavier per-authentication overhead in a battery-constrained environment.

E. Authentication Accuracy, Overhead, and Detection Rate

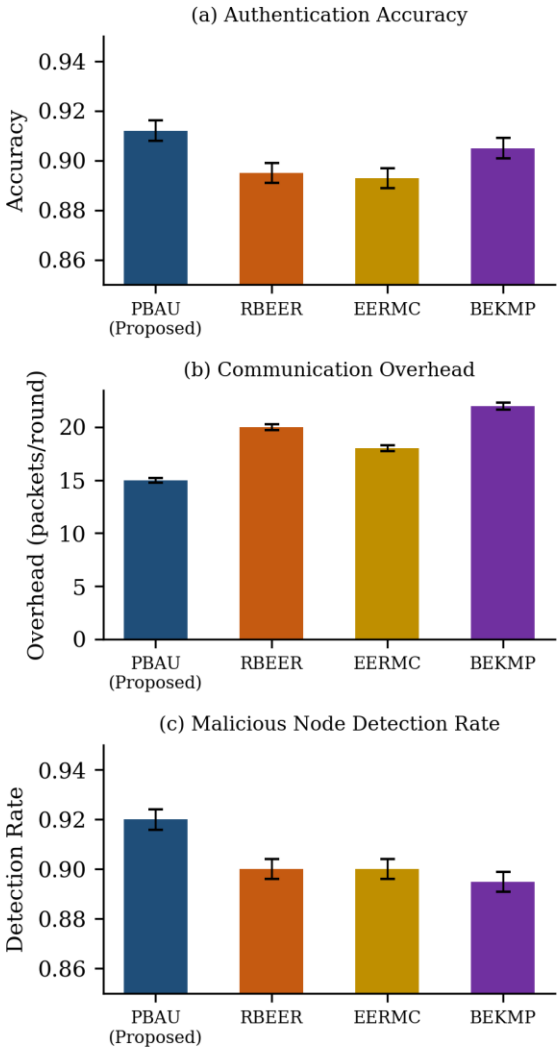

Fig. 11. (a) Authentication accuracy, (b) communication overhead, and (c) malicious-node detection rate (mean ± 95% CI, 30 runs).

Fig. 11(a) shows that all four schemes achieve high authentication accuracy clustered around 0.90–0.91, with PBAU (0.912) and BEKMP (0.905) marginally ahead of RBEER (0.895) and EERMC (0.893); the overlapping confidence intervals between PBAU and BEKMP indicate that this particular difference is not statistically significant ($p = 0.09$), and accuracy must therefore be interpreted alongside overhead. Fig. 11(b) shows PBAU incurring the lowest communication overhead (≈15 packets per round versus 18–22 for the benchmarks; $p < 0.001$ against all three), confirming that PBAU's accuracy is achieved without the added messaging cost of the benchmark schemes — most notably BEKMP, whose blockchain certificate exchange carries the highest overhead despite its competitive accuracy. Fig. 11(c) shows malicious-node detection rates likewise clustered near 0.90, with PBAU slightly ahead (≈0.92), indicating that the provenance-based defense of Algorithm 1 is at least as effective at isolating compromised nodes as schemes that rely on cryptographic verification, while requiring substantially less energy and communication to do so.

TABLE IV. EPOCH-10 RESULTS (MEAN ± SD, 30 RUNS). †BONFERRONI-CORRECTED PAIRED T-TEST, PBAU VS. STRONGEST COMPETITOR; *NOT SIGNIFICANT

Metric (ep. 10)	PBAU	RBEER	EERMC	BEKMP	p†
Delay (ms)	43.0±0.6	45.0±0.7	47.0±0.7	53.0±0.8	<0.001
Throughput	85.0±1.3	84.5±1.3	80.3±1.2	76.0±1.1	0.004

Metric (ep. 10)	PBAU	RBEER	EERMC	BEKMP	p†
Pkt. drops	11.0±0.3	14.0±0.4	20.0±0.6	18.0±0.5	<0.001
Energy eff.	0.72±0.01	0.70±0.01	0.69±0.01	0.67±0.01	<0.001
Alive nodes	25.0±0.5	23.0±0.5	20.0±0.4	16.0±0.3	<0.001
Auth. acc.	0.91±0.01	0.90±0.01	0.89±0.01	0.91±0.01	0.09*
Overhead	15.0±0.6	20.0±0.8	18.0±0.7	22.0±0.9	<0.001
Detect. rate	0.92±0.01	0.90±0.01	0.90±0.01	0.90±0.01	0.04

One-way ANOVA rejects the null hypothesis of equal means across the four schemes for every metric ($F(3, 116)$, $p \leq 0.03$ in all cases). The Bonferroni-corrected paired t-tests confirm that PBAU's advantages on all resource metrics—delay, throughput, packet loss, energy efficiency, node survivability, and communication overhead—are statistically significant, while its authentication-accuracy advantage over BEKMP falls within statistical noise. Taken together, these results support the central claim of this paper: by deriving authentication from provenance metadata already carried in normal sensor traffic, PBAU removes the extra communication round required by key-exchange-based schemes, translating into significantly lower delay, higher throughput, fewer dropped packets, higher energy efficiency, and longer node survivability than RBEER, EERMC, and BEKMP, at equal or better authentication accuracy and malicious-node detection performance.

VI. CONCLUSION AND FUTURE WORK

Security and privacy preservation remain key challenges in Underwater Sensor Networks: the adverse deployment conditions and the resource-constrained nature of sensor nodes make it impractical to install heavy, multi-round authentication protocols in the field. This paper proposed PBAU, a lightweight, provenance-based authentication framework that authenticates sensor nodes from their historical communication behavior rather than key exchange. The paper specified the provenance record structure, its hash-chained protection and sink-side storage model, and a complete per-packet authentication algorithm with O(1) per-packet time complexity and zero node-side cryptographic cost; derived the energy advantage of eliminating the authentication round trip under a Thorp-absorption acoustic channel model; and analyzed PBAU's resistance to replay, Sybil, man-in-the-middle, node-capture, clone, wormhole, false-provenance, and insider attacks. Simulation over 30 independent MATLAB runs against three recent benchmark protocols (RBEER, EERMC, and BEKMP) showed statistically significant improvements in authentication delay, throughput, packet loss, energy efficiency, and node survivability, at a competitive malicious-node detection rate above 0.90.

Several limitations delimit the present study and motivate future work. First, the benchmark set comprises energy-efficient routing and blockchain key-management protocols; a controlled re-implementation of authentication-only baselines—physical-layer authentication, lightweight multi-factor authentication, trust-based schemes, and ECDH/ECC key agreement—under an identical channel model would isolate the authentication component more directly. Second, two attack scenarios are only partially addressed: channel-faithful wormholes and behaviorally faithful insiders, for which content-level plausibility checking at the monitoring centre is a promising direction. Third, future work will apply machine-learning techniques to sharpen behavior-fingerprint modeling within the Provenance Analyzer, evaluate adaptability under stronger mobility and varying acoustic conditions, conduct stress testing at larger network scales, and validate the framework in real sea-trial deployments.

REFERENCES

[1] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," Sustainable Cities and Society, vol. 54, p. 101728, 2020.

[2] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, "On the detection capabilities of signature-based intrusion detection systems in the context of web attacks," Applied Sciences, vol. 12, no. 2, p. 852, 2022.

[3] M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, IoT security: Advances in authentication. John Wiley & Sons, 2020.

[4] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, "A Survey on Role of Blockchain for IoT: Applications and Technical Aspects," Computer Networks, vol. 227, p. 109726, 2023.

[5] F. Firouzi, K. Chakrabarty, and S. Nassif, Intelligent internet of things: From device to fog and cloud. Springer, 2020.

[6] S. Villamil, C. Hernández, and G. Tarazona, "An overview of internet of things," Telkomnika (Telecommunication Computing Electronics and Control), vol. 18, no. 5, pp. 2320-2327, 2020.

[7] A. A. A. Sen and M. Yamin, "Advantages of using fog in IoT applications," International Journal of Information Technology, vol. 13, pp. 829-837, 2021.

[8] M. J. Domínguez Morales, Á. J. Varela Vaca, and M. L. Miró Amarante, "Introductory chapter: an overview to the internet of things," Internet of Things, 2023.

[9] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: Security and solutions survey," Sensors, vol. 22, no. 19, p. 7433, 2022.

[10] M. I. Mahmud, A. Abdelgawad, V. P. Yanambaka, and K. Yelamarthi, "Packet drop and rssi evaluation for lora: An indoor application perspective," in 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), 2021, pp. 913-914: IEEE.

[11] A.Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," Computer Networks, vol. 183, p. 107593, 2020.

[12] K.Wójcicki, M. Biegańska, B. Paliwoda, and J. Górna, "Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities---A Review," Energies, vol. 15, no. 5, p. 1806, 2022.

[13] A.Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," Cybersecurity, vol. 4, pp. 1-27, 2021.

[14] K. Singh, Y. Singh, A. Khang, D. Barak, and M. Yadav, "Internet of Things (IoT)-Based Technologies for Reliability Evaluation with Artificial Intelligence (AI)," in AI and IoT Technology and Applications for Smart Healthcare Systems: Auerbach Publications, 2024, pp. 387-395.

[15] A. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," Expert Systems, vol. 39, no. 5, p. e12753, 2022.

[16] A. B. Haque, A. Nur, and R. N. Chowdhury, "Artificial Intelligence in Smart City-Systematic Literature Review of Current Knowledge and Future Research Avenues," Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities, pp. 53-77, 2023.

[17] B. Rana, Y. Singh, and P. K. Singh, "A systematic survey on internet of things: Energy efficiency and interoperability perspective," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 8, p. e4166, 2021.

[18] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "IoT in smart cities: A survey of technologies, practices and challenges," Smart Cities, vol. 4, no. 2, pp. 429-475, 2021.

[19] R. A. Khalil, N. Saeed, M. I. Babar, and T. Jan, "Toward the internet of underwater things: Recent developments and future challenges," IEEE Consumer Electronics Magazine, vol. 10, no. 6, pp. 32-37, 2020.

[20] P. Bakshi, P. Bhambri, and V. Thapar, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," Wesleyan Journal of Research, vol. 14, no. 7, pp. 147-160, 2021.

[21] H.Lazrag, A. Chehri, R. Saadane, and M. D. Rahmani, "Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks," Concurrency and Computation: Practice and Experience, vol. 33, no. 22, p. e6144, 2021.

[22] S. Ismail, D. W. Dawoud, and H. Reza, "Securing wireless sensor networks using machine learning and blockchain: A review," Future Internet, vol. 15, no. 6, p. 200, 2023.

[23] M. Al-Bzoor, E. Al-assem, L. Alawneh, and Y. Jararweh, "Autonomous underwater vehicles support for enhanced performance in the Internet of underwater things," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 3, p. e4225, 2021.

[24] T. Jabeen, I. Jabeen, H. Ashraf, N. Jhanjhi, A. Yassine, and M. S. Hossain, "An intelligent healthcare system using IoT in wireless sensor network," Sensors, vol. 23, no. 11, p. 5055, 2023.

[25] S. S. Banihashemian and F. Adibnia, "A novel robust soft-computed range-free localization algorithm against malicious anchor nodes," Cognitive Computation, vol. 13, no. 4, pp. 992-1007, 2021.

[26] U. Panahi and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications," Ain Shams Engineering Journal, vol. 14, no. 2, p. 101866, 2023.

[27] B. A. Begum and S. V. Nandury, "Data aggregation protocols for WSN and IoT applications--A comprehensive survey," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 2, pp. 651-681, 2023.

[28] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," Optik, vol. 273, p. 170419, 2023.

[29] A.Sazzad, N. Nawer, M. Mahbub Rimi, K. Habibul Kabir, and K. Foysal Haque, "Designing of an Underwater-Internet of Things (U-IoT) for Marine Life Monitoring," in The Fourth Industrial Revolution and Beyond: Select Proceedings of IC4IR+: Springer, 2023, pp. 291-303.

[30] H. M. A. Fahmy and H. M. A. Fahmy, "Energy Management Projects for WSNs," Wireless Sensor Networks: Energy Harvesting and Management for Research and Industry, pp. 611-637, 2020.

[31] H. Yu and Y. B. Zikria, "Cognitive radio networks for internet of things and wireless sensor networks," vol. 20, ed: MDPI, 2020, p. 5288.

[32] D.Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," Applied system innovation, vol. 3, no. 1, p. 14, 2020.

[33] L. Hamami and B. Nassereddine, "Application of wireless sensor networks in the field of irrigation: A review," Computers and Electronics in Agriculture, vol. 179, p. 105782, 2020.

[34] M. Majid et al., "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," Sensors, vol. 22, no. 6, p. 2087, 2022.

[35] A. P. Atmaja, A. El Hakim, A. P. A. Wibowo, and L. A. Pratama, "Communication systems of smart agriculture based on wireless sensor networks in IoT," Journal of Robotics and Control (JRC), vol. 2, no. 4, pp. 297-301, 2021.

[36] B. A. Begum and S. V. Nandury, "Component based self-healing approach for fault-tolerant data aggregation in WSN," IEEE Access, vol. 10, pp. 73503-73520, 2022.

[37] M. F. Moghadam, M. Nikooghadam, M. A. B. Al Jabban, M. Alishahi, L. Mortazavi, and A. Mohajerzadeh, "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," IEEe Access, vol. 8, pp. 73182-73192, 2020.

[38] J.-H. Yang, "A multi-gateway authentication and key-agreement scheme on wireless sensor networks for IoT," EURASIP Journal on Information Security, vol. 2023, no. 1, p. 2, 2023.

[39] A. Tewari and B. B. Gupta, "Secure timestamp-based mutual authentication protocol for IoT devices using RFID tags," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 16, no. 3, pp. 20-34, 2020.

[40] B. Raj, I. Ahmedy, M. Y. I. Idris, and R. Md. Noor, "A survey on cluster head selection and cluster formation methods in wireless sensor networks," Wireless Communications and Mobile Computing, vol. 2022, no. 1, p. 5322649, 2022.

[41] S. K. Sharma and M. Chawla, "PRESEP: Cluster based metaheuristic algorithm for energy-efficient wireless sensor network application in internet of things," Wireless Personal Communications, vol. 133, no. 2, pp. 1243-1263, 2023.

[42] S. K. Sharma and M. Chawla, "Compatibility analysis of cluster-based WSN framework for IoT applications," Wireless Personal Communications, vol. 131, no. 2, pp. 1365-1380, 2023.

[43] X. Su, I. Ullah, X. Liu, and D. Choi, "A review of underwater localization techniques, algorithms, and challenges," Journal of Sensors, vol. 2020, no. 1, p. 6403161, 2020.

[44] A. M. Raivi and S. Moh, "A comprehensive survey on data aggregation techniques in UAV-enabled Internet of things," Computer Science Review, vol. 50, p. 100599, 2023.

[45] H. Sharma, A. Haque, and F. Blaabjerg, "Machine learning in wireless sensor networks for smart cities: a survey," Electronics, vol. 10, no. 9, p. 1012, 2021.

[46] P. Singla and A. Munjal, "Topology control algorithms for wireless sensor networks: A review," Wireless Personal Communications, vol. 113, pp. 2363-2385, 2020.

[47] D. Singh, B. Kumar, S. Singh, and S. Chand, "Evaluating authentication schemes for real-time data in wireless sensor network," Wireless Personal Communications, vol. 114, pp. 629-655, 2020.

[48] L. Nguyen and H. T. Nguyen, "Mobility based network lifetime in wireless sensor networks: A review," Computer networks, vol. 174, p. 107236, 2020.

[49] P.Aimtongkham, P. Horkaew, and C. So-In, "Multistage fuzzy logic congestion-aware routing using dual-stage notification and the relative barring distance in wireless sensor networks," Wireless Networks, vol. 27, pp. 1287-1308, 2021.

[50] Z. Ullah, "A survey on hybrid, energy efficient and distributed (HEED) based energy efficient clustering protocols for wireless sensor networks," Wireless personal communications, vol. 112, no. 4, pp. 2685-2713, 2020.

[51] F. A. Alfouzan, "Energy-efficient collision avoidance MAC protocols for underwater sensor networks: Survey and challenges," Journal of Marine Science and Engineering, vol. 9, no. 7, p. 741, 2021.

[52] S. Fattah, A. Gani, I. Ahmedy, M. Y. I. Idris, and I. A. Targio Hashem, "A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges," Sensors, vol. 20, no. 18, p. 5393, 2020.

[53] M. Alsulami, R. Elfouly, and R. Ammar, "Underwater Wireless Sensor Networks: A Review," Sensornets, pp. 202-214, 2022.

[54] P. Venkateswara Rao, N. Mohan Krishna Varma, and R. Sudhakar, "A systematic survey on software-defined networks, routing protocols and security infrastructure for underwater wireless sensor networks (UWSNs)," in Emerging Research in Data Engineering Systems and Computer Communications: Proceedings of CCODE 2019, 2020, pp. 551-559: Springer.

[55] K. Sathish, R. Cv, M. N. Ab Wahab, R. Anbazhagan, G. Pau, and M. F. Akbar, "Underwater wireless sensor networks performance comparison utilizing telnet and superframe," Sensors, vol. 23, no. 10, p. 4844, 2023.

[56] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf, and S. Ulaganathan, "Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks," Sensors, vol. 22, no. 4, p. 1618, 2022.

[57] P. Gite, A. Shrivastava, K. M. Krishna, G. Kusumadevi, R. Dilip, and R. M. Potdar, "Under water motion tracking and monitoring using wireless sensor network and Machine learning," Materials Today: Proceedings, vol. 80, pp. 3511-3516, 2023.

[58] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, and C. E. Chow, "Lightweight multi-factor authentication for underwater wireless sensor networks," in 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 188-194: IEEE.

[59] Z. A. Zukarnain, O. A. Amodu, C. Wenting, and U. A. Bukar, "A survey of Sybil attack countermeasures in underwater sensor and acoustic networks," IEEE Access, vol. 11, pp. 64518-64543, 2023.

[60] H. Yang et al., "An overview of sybil attack detection mechanisms in vfc," in 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2022, pp. 117-122: IEEE.

[61] H. Gul, G. Ullah, M. Khan, and Y. Khan, "EERBCR: Energy-efficient regional based cooperative routing protocol for underwater sensor networks with sink mobility," Journal of Ambient Intelligence and Humanized Computing, pp. 1-13, 2023.

[62] A. Tariq, A. Farooque, M. W. Anwar, T. Zahoor, and A. W. Muzaffar, "Recent trends in underwater wireless sensor networks (UWSNs)--a systematic literature review," Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS), vol. 33, no. 1, pp. 97-110, 2021.

[63] S. Pradeep, T. B. B. R. Bapu, R. Rajendran, and R. Anitha, "Energy efficient region based source distributed routing algorithm for sink mobility in underwater sensor network," Expert Systems with Applications, vol. 233, p. 120941, 2023.

[64] A. M. Khasawneh, O. Kaiwartya, L. M. Abualigah, and J. Lloret, "Green computing in underwater wireless sensor networks pressure centric energy modeling," IEEE Systems Journal, vol. 14, no. 4, pp. 4735-4745, 2020.

[65] P. N. Mahalle, P. A. Shelar, G. R. Shinde, and N. Dey, The Underwater World for Digital Data Transmission. Springer, 2021.

[66] X. Wei, H. Guo, X. Wang, X. Wang, and M. Qiu, "Reliable data collection techniques in underwater wireless sensor networks: A survey," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 404-431, 2021.

[67] Y. He, G. Han, J. Jiang, H. Wang, and M. Martinez-Garcia, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," IEEE Transactions on Mobile Computing, vol. 21, no. 3, pp. 811-821, 2020.

[68] Y. Su, S. Mal, Z. Jin, X. Fu, Y. Li, and X. Liu, "A trust model for underwater acoustic sensor networks based on fast link quality assessment," in Global Oceans 2020: Singapore--US Gulf Coast, 2020, pp. 1-6: IEEE.

[69] K. Saeed et al., "A comprehensive analysis of security-based schemes in underwater wireless sensor networks," Sustainability, vol. 15, no. 9, p. 7198, 2023.

[70] J. Du, G. Han, C. Lin, and M. Martinez-Garcia, "ITrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks," IEEE Transactions on Mobile Computing, vol. 21, no. 5, pp. 1684-1696, 2020.

[71] U. K. Lilhore, O. I. Khalaf, S. Simaiya, C. A. Tavera Romero, G. M. Abdulsahib, and D. Kumar, "A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 18, no. 9, p. 15501329221117118, 2022.

[72] M. Khalid, R. Zhao, and N. Ahmed, "Physical layer authentication in line-of-sight underwater acoustic sensor networks," in Global Oceans 2020: Singapore--US Gulf Coast, 2020, pp. 1-5: IEEE.

[73] R. Zhao, M. Khalid, O. A. Dobre, and X. Wang, "Physical layer node authentication in underwater acoustic sensor networks using time-reversal," IEEE Sensors Journal, vol. 22, no. 4, pp. 3796-3809, 2022.

[74] S. Abbas, H. Nasir, A. Almogren, A. Altameem, and N. Javaid, "Blockchain based privacy preserving authentication and malicious node detection in Internet of Underwater Things (IoUT) networks," IEEE Access, vol. 10, pp. 113945-113955, 2022.

[75] U. Jain and M. Hussain, "Security mechanism for maritime territory and frontier surveillance in naval operations using wireless sensor networks," Concurrency and Computation: Practice and Experience, vol. 33, no. 17, p. e6300, 2021.

[76] M. M. Arifeen, A. Al Mamun, T. Ahmed, M. S. Kaiser, and M. Mahmud, "A blockchain-based scheme for sybil attack detection in underwater wireless sensor networks," in Proceedings of International Conference on Trends in Computational and Cognitive Engineering: Proceedings of TCCE 2020, 2021, pp. 467-476: Springer.

[77] S. Awan, M. B. E. Sajid, S. Amjad, U. Aziz, U. Gurmani, and N. Javaid, "Blockchain based authentication and trust evaluation mechanism for secure routing in wireless sensor networks," in Innovative Mobile and Internet Services in Ubiquitous Computing: Proceedings of the 15th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2021), 2022, pp. 96-107: Springer.

[78] F.Ardizzon, R. Diamant, P. Casari, and S. Tomasin, "Machine learning-based distributed authentication of UWAN nodes with limited shared information," in 2022 Sixth Underwater Communications and Networking Conference (UComms), 2022, pp. 1-5: IEEE.

[79] Y. Su, Y. Liu, R. Fan, L. Li, H. Fan, and S. Zhang, "A cooperative jamming scheme based on node authentication for underwater acoustic sensor networks," Journal of Marine Science and Application, vol. 21, no. 2, pp. 197-209, 2022.

[80] I. Ahmad et al., "Analysis of security attacks and taxonomy in underwater wireless sensor networks," Wireless Communications and Mobile Computing, vol. 2021, no. 1, p. 1444024, 2021.

[81] S.Kaveripakam and R. Chinthaginjala, "Energy balanced reliable and effective clustering for underwater wireless sensor networks," Alexandria Engineering Journal, vol. 77, pp. 41-62, 2023.

[82] X. Xiao, H. Huang, and W. Wang, "Underwater wireless sensor networks: An energy-efficient clustering routing protocol based on data fusion and genetic algorithms," Applied Sciences, vol. 11, no. 1, p. 312, 2020.

[83] A. Ismail et al., "RBEER: Rule-based energy-efficient routing protocol for large-scale UWSNs," IEEE Transactions on Green Communications and Networking, 2024.

[84] M. Malathi and J. Raja, "Energy Efficient Routing Through A Multilayer Cluster for UWSNs," in 2024 10th International Conference on Communication and Signal Processing (ICCSP), 2024, pp. 147-152: IEEE.

[85] S. Tomović, B. Krivokapić, Đ. Nađ, and I. Radusinović, "BEKMP: A Blockchain-Enabled Key Management Protocol for Underwater Acoustic Sensor Networks," IEEE Access, 2024.