Sri Lanka Institute of Information Technology

Security Challenges in Internet of Underwater Things

Student Name – Wanasinghe N.K

Student ID – IT23221000

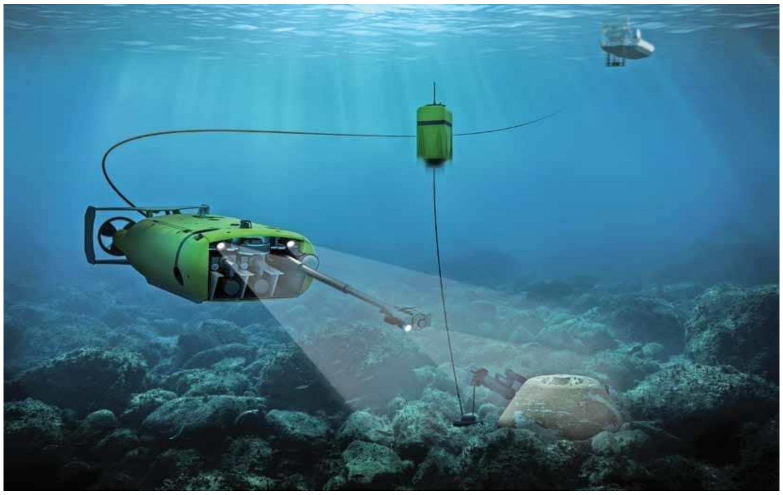
Introduction to Cyber Security – IE2022

B.Sc. (Hons) in information Technology Specializing in Cyber Security

Table of Contents

Abstract

While the Earth is covered with 71% of water, a significant portion of the underwater environment remains unexplored due to lack of various technological constraints. One technology that has been developed to address this problem is The Internet of Underwater Things (IoUT). It is an advanced network consisting of smart devices that can operate underwater. IoUT is effective in a very broad area such as environmental monitoring of the oceans as well as tunnel construction. Such technology is beneficial to the society since it can enhance the knowledge and management of the ocean, which is critical in tackling global problems like climate change and resource consumption. These networks are difficult to secure due to the characteristics of underwater audio communication, limited bandwidth, complex latency, surrounding dynamic environment of operational sensors and underwater device resources constraints.



This work is dedicated to the study of IoUT and Underwater Wireless Sensor Networks (UWSNs), with considerable attention to the underwater environment and consideration of its key security challenges to the security. Most of these situations are related to **attacks such as jamming, Wormhole, Sybil, sinkhole, blackhole, spoofing and flooding attacks**.

This report further investigates countermeasures to prevent such attacks as improving existing algorithms, making use of cryptographic tools, and applying machine learning models. **An important outcome of this study is the identification of the main security challenges of IoUT and UWSN systems with vulnerabilities and proposing mitigation strategies to build solid defenses to establish a set of guidelines and practices to ensure confidentiality, authentication, integrity, and availability of information**.

Introduction

Water is the basis of life and a need for all people around the world. However, it has been an increasingly limited and reduced natural resource for millions of the world's populations [1]. Security in underwater involves the defense of underwater sensor networks, communications against data leakage, signal jamming, and cyber-attacks. As a result, the issue of how to protect underwater communication systems is getting more interested in general cybersecurity as well.

According to the GHD analysis, about a quarter of global water systems will likely have experienced a cybersecurity breach by 2025 [2]. Therefore, underwater security is an important factor to be considered.

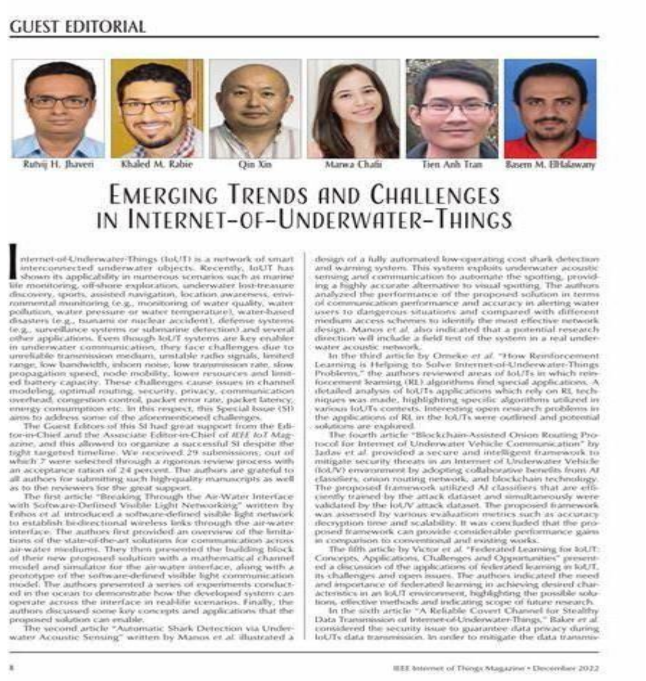
Different types of cyber-attacks present a threat to the underwater communication systems' integrity. The common occurrence in this issue requires strong security measures within the Internet of Underwater Things. Enhancements in audio communication and sensor technologies of Underwater Wireless Sensor Networks results in introducing IoUT for underwater condition monitoring [3]. To explore into the domain of Underwater Wireless Sensor Networks, it is required to first define the Internet of Underwater Things.

What is Internet of Underwater Things (IoUT)?

Smart city evolution has become more and more popular in recent years. The Internet of Things (IoT), which is referred to as "The infrastructure of the information society," [4] is one of the most critical strategies to implement. The idea behind this was originally introduced in 1985 [4], while the Internet of Underwater Things (IoUT) was first mentioned in 2012 [5]. "The network of smart interconnected underwater objects" is the definition of IoUT.

Underwater smart objects may consist of various kinds of underwater sensors, ships, buoys, autonomous surface vehicles (ASVs), autonomous underwater vehicles (AUVs), etc. IoUT, an innovative kind of IoT, is crucial to the development of smart cities.

Therefore, the term IoUT describes a network consisting of sensors and



GUEST EDITORIAL

Rutvij H. Jhaveri Khaled M. Rabie Qin Xin Marwa Chafii Tien Anh Tran Basem M. ElHalawany

EMERGING TRENDS AND CHALLENGES IN INTERNET-OF-UNDERWATER-THINGS

Internet-of-Underwater-Things (IoUT) is a network of smart interconnected underwater objects. Recently, IoUT has shown its applicability in numerous scenarios such as marine life monitoring, off-shore exploration, underwater lost-treasure discovery, sports, assisted navigation, location awareness, environmental monitoring (e.g., monitoring of water quality, water pollution, water pressure or water temperature), water-based disasters (e.g., tsunami or nuclear accident), defense systems (e.g., surveillance systems or submarine detection) and several other applications. Even though IoUT systems are key enabler in underwater communication, they face challenges due to unreliable transmission medium, unstable radio signals, limited range, low bandwidth, inborn noise, low transmission rate, slow propagation speed, node mobility, lower resources and limited battery capacity. These challenges cause issues in channel modeling, optimal routing, security, privacy, communication overhead, congestion control, packet error rate, packet latency, energy consumption etc. In this respect, this Special Issue (SI) aims to address some of the aforementioned challenges.

The Guest Editors of this SI had great support from the Editor-in-Chief and the Associate Editor-in-Chief of *IEEE IoT Magazine*, and this allowed to organize a successful SI despite the tight targeted timeline. We received 29 submissions; out of which 7 were selected through a rigorous review process with an acceptance ration of 24 percent. The authors are grateful to all authors for submitting such high-quality manuscripts as well as to the reviewers for the great support.

The first article "Breaking Through the Air-Water Interface with Software-Defined Visible Light Networking" written by Enhos et al. introduced a software-defined visible light network to establish bi-directional wireless links through the air-water interface. The authors first provided an overview of the limitations of the state-of-the-art solutions for communication across air-water mediums. They then presented the building block of their new proposed solution with a mathematical channel model and simulator for the air-water interface, along with a prototype of the software-defined visible light communication model. The authors presented a series of experiments conducted in the ocean to demonstrate how the developed system can operate across the interface in real-life scenarios. Finally, the authors discussed some key concepts and applications that the proposed solution can enable.

The second article "Automatic Shark Detection via Underwater Acoustic Sensing" written by Manos et al. illustrated a design of a fully automated low-operating cost shark detection and warning system. This system exploits underwater acoustic sensing and communication to automate the spotting, providing a highly accurate alternative to visual spotting. The authors analyzed the performance of the proposed solution in terms of communication performance and accuracy in alerting water users to dangerous situations and compared with different medium access schemes to identify the most effective network design. Manos et al. also indicated that a potential research direction will include a field test of the system in a real underwater acoustic network.

In the third article by Omeke *et al.* "How Reinforcement Learning is Helping to Solve Internet-of-Underwater-Things Problems," the authors reviewed areas of IoUTs in which reinforcement learning (RL) algorithms find special applications. A detailed analysis of IoUTs applications which rely on RL techniques was made, highlighting specific algorithms utilized in various IoUTs contexts. Interesting open research problems in the applications of RL in the IoUTs were outlined and potential solutions are explored.

The fourth article "Blockchain-Assisted Onion Routing Protocol for Internet of Underwater Vehicle Communication" by Jadav et al. provided a secure and intelligent framework to mitigate security threats in an Internet of Underwater Vehicle (IoUV) environment by adopting collaborative benefits from AI classifiers, onion routing network, and blockchain technology. The proposed framework utilized AI classifiers that are efficiently trained by the attack dataset and simultaneously were validated by the IoUV attack dataset. The proposed framework was assessed by various evaluation metrics such as accuracy decryption time and scalability. It was concluded that the proposed framework can provide considerable performance gains in comparison to conventional and existing works.

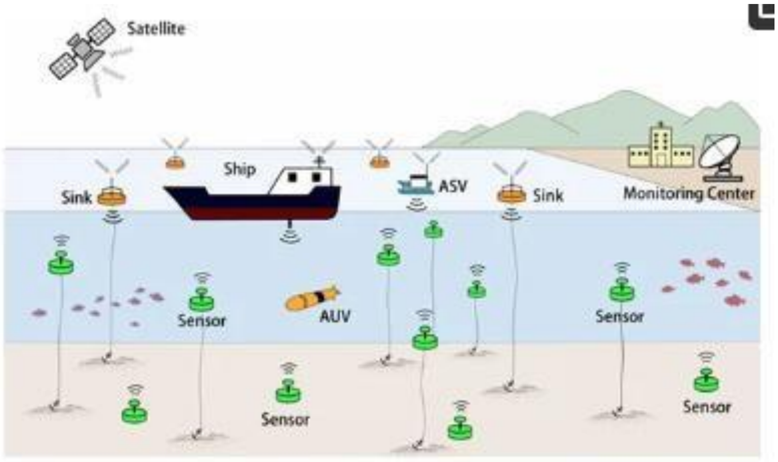
The fifth article by Victor et al. "Federated Learning for IoUT: Concepts, Applications, Challenges and Opportunities" presented a discussion of the applications of federated learning in IoUT, its challenges and open issues. The authors indicated the need and importance of federated learning in achieving desired characteristics in an IoUT environment, highlighting the possible solutions, effective methods and indicating scope of future research.

In the sixth article "A Reliable Covert Channel for Stealthy Data Transmission of Internet-of-Underwater-Things," Baker *et al.* considered the security issue to guarantee data privacy during IoUTs data transmission. In order to mitigate the data transmis-

8 IEEE Internet of Things Magazine • December 2022

underwater devices that gather and share data in order to monitor and control underwater surroundings. IoUT improves the understanding and the capacity to engage with marine ecosystems through remote sensing and data analysis, much like the Internet of Things (IoT) on land.

UWSNs, which are made up of stationary or mobile nodes that communicate via sound waves, are used by IoUT. Technological improvements continue to launch the development and distribution of IoUT solutions despite the difficulties presented by the undersea environment, including restricted communication capabilities, high energy consumption, and security vulnerabilities, making it an essential field of research and marine studies.



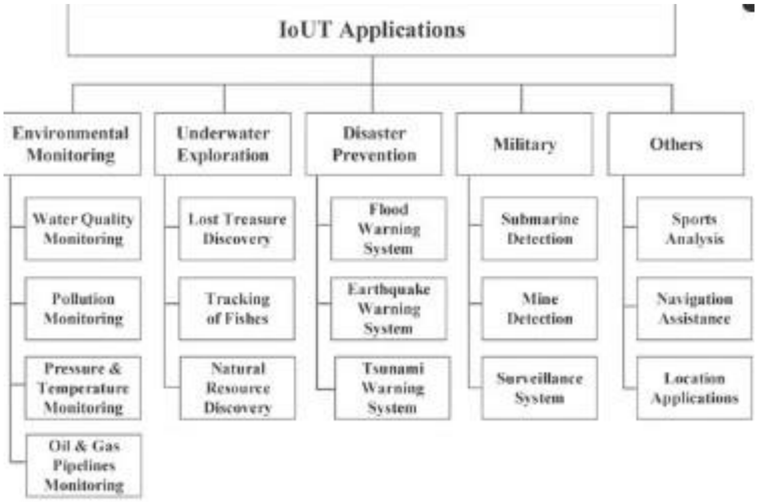
What are the applications of IoUT?

Environmental Monitoring: using wireless sensor networks, IoUT makes it possible to continuously monitor chemical pollution, oil and gas pipeline surveillance and water quality in rivers and pipelines.

Underwater research: Using AUVs and UWSNs for mineral and coral resource research makes treasure hunting and resource tracking easier.

Disaster Prevention: IoUT improves disaster response by providing early warning systems for tsunamis and floods through real-time monitoring networks.

Military Applications: By distributing sensors effectively, IoUT enhances defensive and surveillance tactics for the purpose of detecting submarines and mines [7].



Challenges in IoUT

Media of Transmission: Thus, for communications, while Underwater Wireless Sensor Networks depend on audio signals as radio signals are rapidly absorbed in water, terrestrial wireless sensor networks use radio waves.

The imbalance of UWSNs and TWSNs is that TWSN specific communication protocols usually perform better than communication protocols designed for UWSN.

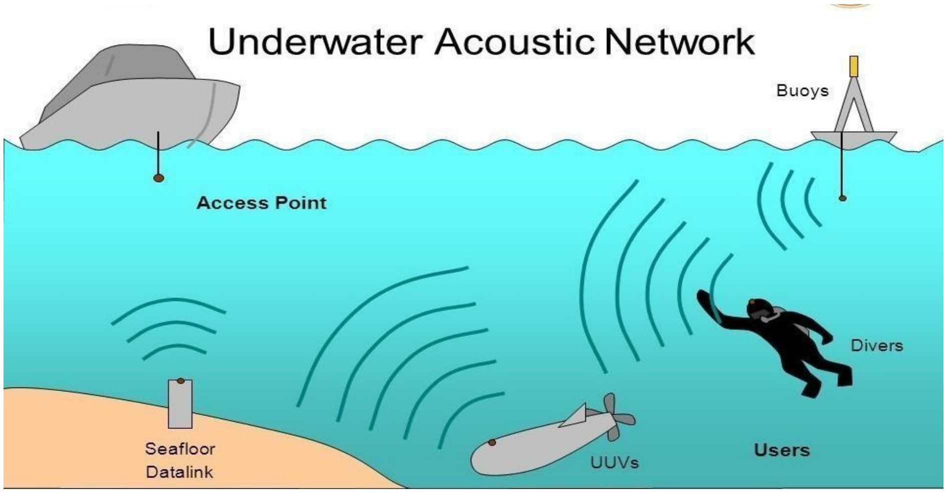
Speed of Propagation: UWSN signals have a propagation speed of 1500m/s compared to TWSNs, where signals move at a speed of 300,000,000 m/s. Due to such differences, it may take more time for a certain node to send a certain amount of data [7].

Rate of Transmission: Poor transmission rates of communication around 10 kilobits per second, through the use of audio in UWSNs are due to its limited bandwidth. Because of this, using bandwidth efficiently becomes crucial.

Having Trouble Recharging: Because underwater sensors are sunken, recharging them is challenging, which brings questions regarding energy efficiency.

Mobility: UWSNs naturally movable due to water currents making control of the dynamic network structures more difficult.

Reliability: Due to noise from the surroundings such as ship noise or turbulence from the water and transmission loss (signal fading), the connections in UWSNs have low and inconsistent reliability.
longer delays and increased energy consumption can result from frequent data retransmissions due to low reliability [7].



Moreover, the above studies show that Underwater Wireless Sensor Networks used by IoUT are highlighted most often and most of the mentioned challenges are associated with UWSNs.

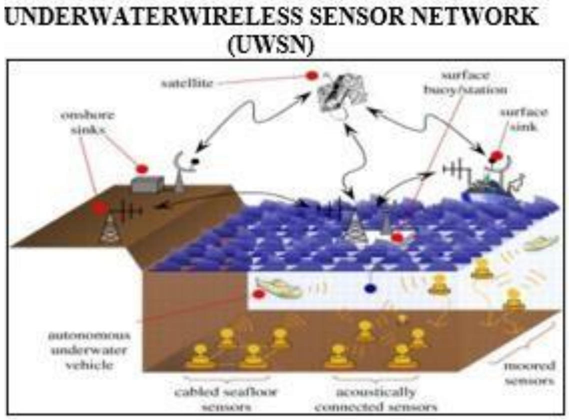
What are Underwater Wireless Sensor Networks (UWSN)?

A massive part of ocean research is managed by locating sensors to measure water temperature, speed, pressure, and chemicals of the ocean. The collected data from the sensors are physically retrieved and downloaded for analyzing purposes. This approach does not produce real-time data analysis, which is essential for predictions. This challenge introduces the essentiality of Underwater Wireless Sensor Networks [8].

As a result, the possible usage of UWSNs to monitor and investigate underwater environments. Underwater sensors are used by these networks to gather data, which is then transmitted in real time via advanced communication technologies. UWSNs are improved by the IoUT, a subset of IoT, which facilitates intelligent marine activities like undersea exploration, maritime navigation, and disaster predictions [9].

Characteristics of UWSNs

According to Das and Thampi, “Most current wireless sensor network security protocols assume sensor networks as stationary (not moving). Moreover, the network performance reduces with the addition of security techniques” [10]. This comment highlights a common feature of most of the security mechanisms designed for Wireless Sensor Networks (WSNs) which is that the designers assume that the sensors in the network do not move. Water currents tend to make the sensors in UWSNs movable. The same security mechanisms of WSNs cannot be implemented to UWSNs since they were not designed for networks with moving nodes.


UNDERWATERWIRELESS SENSOR NETWORK (UWSN)
satellite
surface buoy/station
onshore sinks
surface sink
autonomous underwater vehicle
cabled seafloor sensors
acoustically connected sensors
moored sensors

Communication Channel

Compared to WSNs, which use radio waves for communication, UWSNs use sound waves or acoustic signals to communicate in an underwater environment [11].
These factors result in less efficient data capacity, slower transmission and a high number of errors in underwater.
Therefore, the sound waves used in UWSNs are more vulnerable to attacks since the sound waves spread in the open water and not in a restricted location [10].

Environment of Operation

Since ocean currents cause the sensors' positions to change, the network's structure is always changing.
As a result, these changes disrupt the process of safe and correct transmission of the data [11]. Moreover, they emphasize the need for secured and accurate sensor placements and time synchronization [12].

Energy and Hardware

UWSNs cannot be easily maintained or recharged because they are deployed underwater, whereas WSNs can be charged using solar power [11]. This further increases energy restrictions, which affects security by limiting the variety of security measures available.

With the discussion of the above characteristics of UWSNs, the security field in this area is rather challenging and complex due to factors such as dynamic nature of the network, limited power resources, lack of a secure communication channel, lack of secure localization and synchronization. These situations require special security mechanisms that are different from traditional Wireless Sensor Networks.

Evolution of the topic

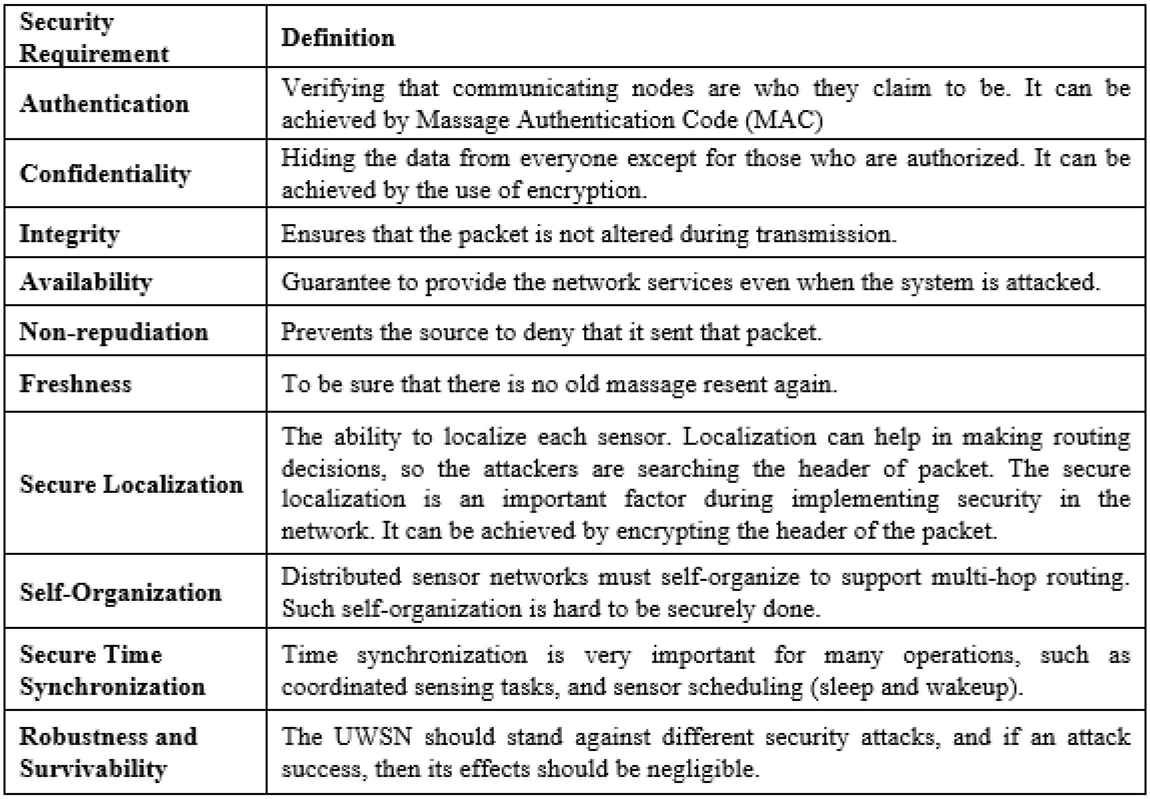
Security in UWSNs

Protecting UWSNs from threats is a major concern because the characteristics of these networks result in certain limited security aspects. While WSNs have generated many research sessions focused on the security area, it is limited to UWSNs. The reason for that is the difficulty of satisfying security requirements in UWSNs due to the unique restrictions of the underwater environment. Moreover, the nodes in UWSNs have limited processing power, memory space, restricted bandwidth and limited power. Therefore, security services in UWSNs should ensure the protection of the data maintained in the network.

Security Requirements

To ensure safety in UWSNs, security criteria must be put forward. The following table provides all the security requirements related to UWSNs.

Table 1: The security requirement of UWSNs [13].



Security Requirement	Definition
Authentication	Verifying that communicating nodes are who they claim to be. It can be achieved by Massage Authentication Code (MAC)
Confidentiality	Hiding the data from everyone except for those who are authorized. It can be achieved by the use of encryption.
Integrity	Ensures that the packet is not altered during transmission.
Availability	Guarantee to provide the network services even when the system is attacked.
Non-repudiation	Prevents the source to deny that it sent that packet.
Freshness	To be sure that there is no old massage resent again.
Secure Localization	The ability to localize each sensor. Localization can help in making routing decisions, so the attackers are searching the header of packet. The secure localization is an important factor during implementing security in the network. It can be achieved by encrypting the header of the packet.
Self-Organization	Distributed sensor networks must self-organize to support multi-hop routing. Such self-organization is hard to be securely done.
Secure Time Synchronization	Time synchronization is very important for many operations, such as coordinated sensing tasks, and sensor scheduling (sleep and wakeup).
Robustness and Survivability	The UWSN should stand against different security attacks, and if an attack success, then its effects should be negligible.

Security Threats

The significance of UWSNs leads to their security being highly vulnerable, especially due to the broadcast nature of the transmission medium. The low power, limited processing resources and insufficient memory space of UWSN nodes make them vulnerable to number of attacks, reducing their lifespan. Moreover, the high bit error rate during transmission, propagation delay and low bandwidth in terms of the acoustic communication channel exposes UWSNs to communication and manipulation attacks [12].

Security Attacks

Attacks on UWSNs can affect reliability, availability and confidentiality of the nodes and the information they gather.

Sensor node Compromise - Sensor Node Compromise: In UWSNs, attackers compromise the node hardware or use the nodes to store data to get information from it. A compromised node will send fake messages with a malicious intent to manipulate or disrupt the operations of a network. [13].

Routing Attacks - In such complex attacks, the compromised nodes may use internal attacks using the protocols used in the network such as routing protocols. Most of the vulnerabilities regarding the routing protocols are due to the absence of authenticity checks, freshness and integrity of the routing information [13].

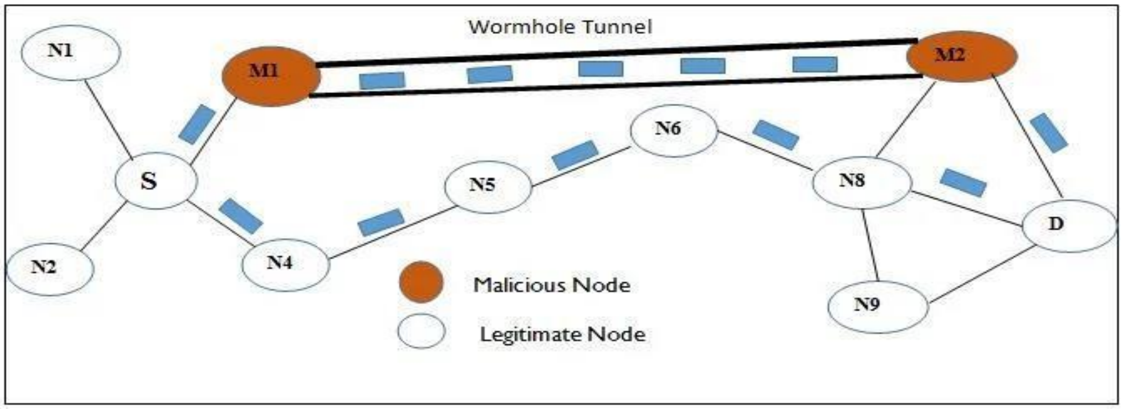
Denial of Service Attacks –DOS attacks are the main attack type that UWSNs can be exposed to, and these attacks can be quite damaging to UWSNs because the movements are simply flooding the network with excessive traffic or countless requests and restrict the normal operational flow. In addition, limited power and bandwidth add to the high error rates that make underwater DoS attacks hard to detect and prevent.

Types of Routing attacks in UWSNs

Wormhole Attack

In UWSNs, a wormhole attack is a critical network layer attack where the attacker creates a malicious communication tunnel through several compromised nodes. These compromised nodes spread data packets through the wormhole, tricking other nodes by giving the impression that they are nearer than they actually are. This affects the normal communication and routing protocols employed. In addition, the malicious nodes can also adjust the data packets or even delete them, putting the network at risk [17].

The biggest challenge in Wormhole attacks is that it is a passive attack. That means it is extremely difficult to detect. The attackers do not need to have any structural knowledge of the network or disrupt any operational nodes to perform these attacks, making them very threatening to networks like UWSNs [18].



Types of Wormhole Attacks in UWSNs

- Open Wormhole

Data packets get tunneled between two wormhole nodes with other nodes bypassing the network.

Other legitimate nodes are avoided on the routing path, making the communication unstable

- Half-Open Wormhole

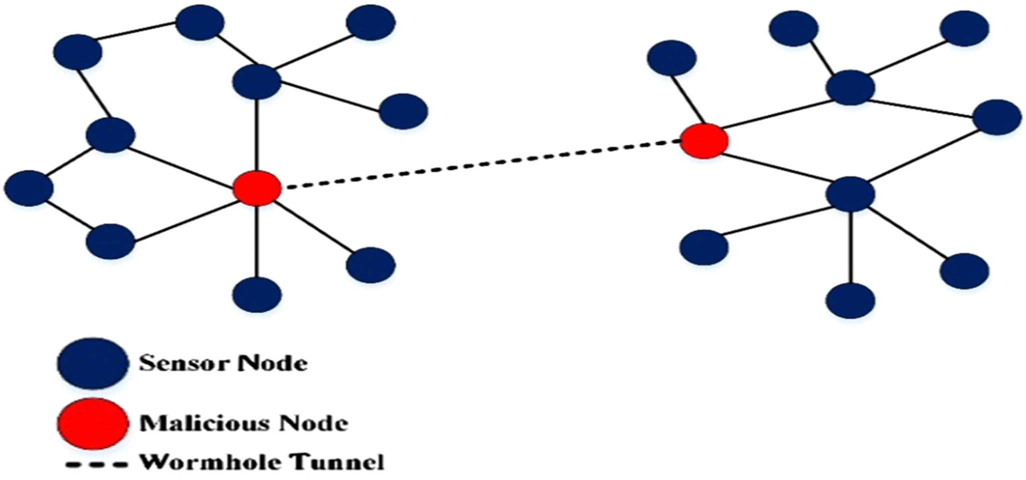
The attacker forwards packets directly to the destination, bypassing intermediate nodes.

This will develop an appearance of a much shorter path, which may disrupt routing protocols.

- Closed Wormhole

It transmits data directly between the source and destination in one hop. It gives an impression of neighboring nodes when they are not.

Because of this, it gives topology errors in the network, causing misrouting [17].



Consequences of wormhole attacks in UWSNs

Data integrity problems: malicious nodes could alter packets that contain sensitive information, resulting in unauthorized access to the sensitive information.

Network Partition: most of the middle nodes are avoided, which results in the scenario of splintering of the network.

System vulnerabilities: Leads to potential other attacks such as eavesdropping, message deception and node impersonation.

Reduced network life span: Since there is uneven energy usage, it leads to depletion of some nodes while other nodes still have charge, and it causes early failure of the network.

Performance impact: This attack causes disturbance in routing, for example, delays the communication that may lead to the reduction of the network throughput.

Countermeasures against Wormhole Attacks in UWSNs

- **Watchdog Model**

Node will constantly monitor the behavior of all intermediate nodes regarding data forwarding. If the node does not relay data within the specified time, then that node is labeled malicious.

The model also fails to handle combined attacks like selective forwarding.

- **Delphi Technique**

This technique calculates the delay per hop and higher delays indicate the presence of a wormhole attack.

Low power and low efficiency due to the presence of many wormholes as average delay increases in the entire network.

- **WRHT-Wormhole Resistant Hybrid Technique**

Hybrid watchdog and Delphi are combined to monitor data loss and also hop delays for increased accuracy in detection.

- **Partial Route Discovery Algorithm**

Discovers multiple routes between nodes in order to verify the smallest route and detect the presence of wormholes.

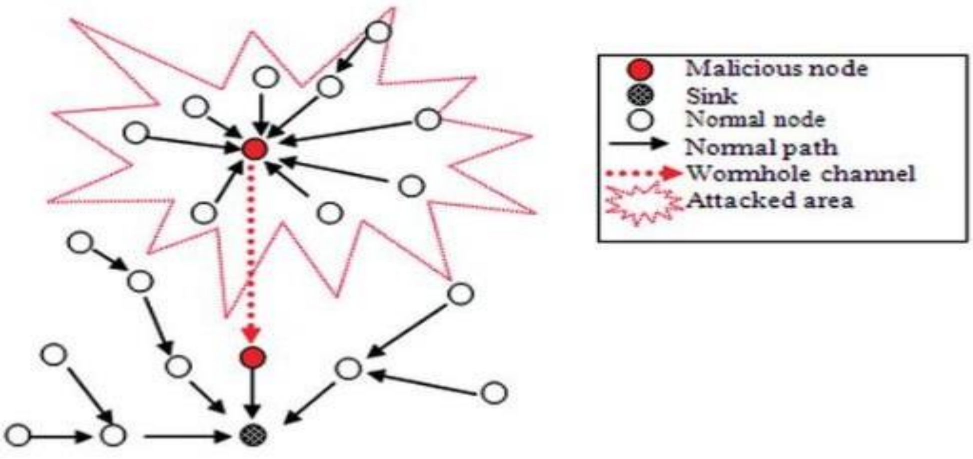
- **Packet Leashes**

Distance of packet transmission is restricted, so that tunneling of packets is not possible.

Types:

Geographical Leash: This limits how far packets can travel in each hop.

Temporal Leash: Bounds total distance for a packet over any number of hops [17].



Sybil Attack

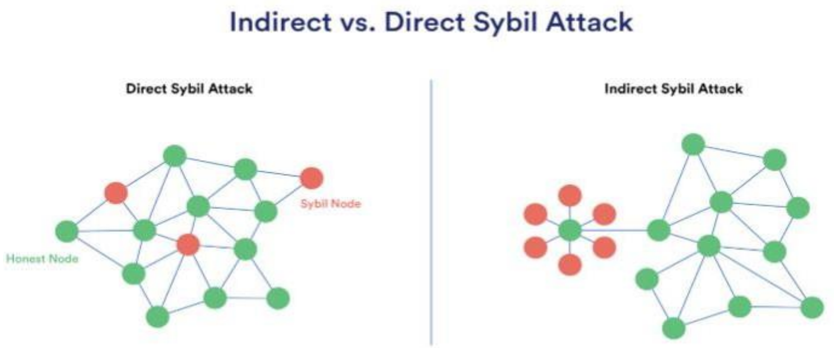
Sybil attack is a severe security threat in UWSNs, and it is an attack in which a malicious node illegitimately claims several identities within the network. In here, the routing and data exchange protocols are manipulated to misroute data and exhaust the resources in order to disturb the communication within the network. These kinds of attacks pose serious risks in UWSNs because usually, nodes have limited resources, and communication is more challenging due to water disruption that has negative consequences on performance, energy efficiency, and security [19].

Types of Sybil attacks in UWSNs

- Direct vs. Indirect Sybil Attack

Direct: This kind of a sybil approach consists of a malicious node directly communicating either with a target node, or legitimate nodes employing multiple identities.

Indirect: The attacker employs other exploited nodes in the network to execute the transmission of his fake identity [19].



- Fabricated vs. Stolen Identities

Fabricated: This is where malicious nodes generate other types of identities suddenly.

Stolen: The attacker steals the identities of legitimate nodes within the network.

- Simultaneous vs. Sequential Sybil Attack

Simultaneous: A malicious node deploys numerous identities at the same time.

Sequential: An attacker deploys one identity at one time and switches to another identity at another time to avoid detection.

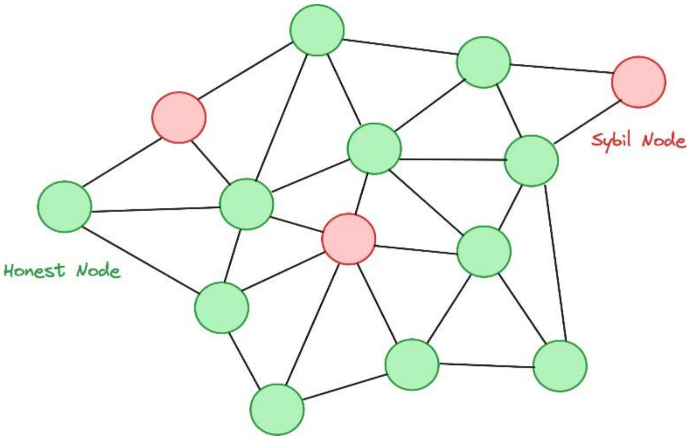
Countermeasures against Sybil attacks in UWSNs

- Trust Models

Define trust levels based on the behavior of nodes to minimize the influence of illegitimate nodes.

- Identity Verification

Use physical layer characteristics such as the signal patterns to authenticate the nodes.



- Reputation Systems

Keep a record of every node's activity over time and detect any suspicious activities from this record [19].

Sinkhole Attack

Sinkhole attack in UWSNs occur when an intruder node compromises an existing node or injects an illegitimate node into the network. This malicious node advertises itself as the best route to the base station. Consequently, it tricks nearby nodes to forward their data packets via itself. Then it attracts not only the nodes closer to it but also those closer to the base station. After that, the intruder can easily modify or drop the data, which will affect the security of the network.

These types of attacks can be initiated inside a network through some compromised node or from outside using some powerful external device [12] [20].

Detection and Prevention Techniques of Sinkhole attacks

- Anomaly Detection

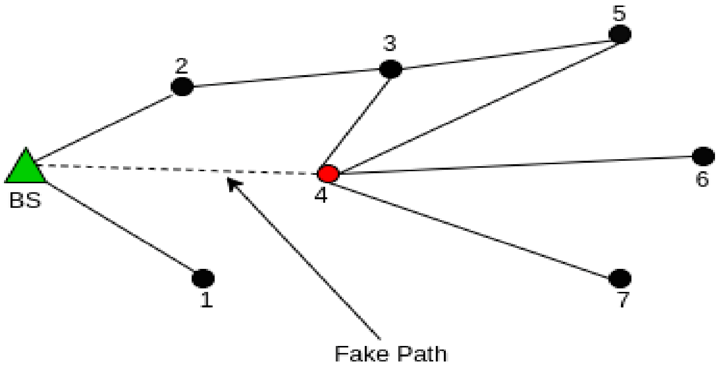
Its purpose is to examine the normal and abnormal behavior of the nodes. However, false alarms can still occur due to this technique.

Disadvantages: It is not very effective in detecting the sinkhole attack and may detect false positives.

- Rule/Signature-Based Detection

It sets policies for the behavior of the nodes. If a node disobeys these policies, the detection system will label the specific node as a malicious node.

Disadvantages: This technique applies and detects attacks of known types only. Its level of effectiveness is low to new attacks [20].



- Statistical Detection

It detects data from node actions such as their CPU usage and packet transfers to determine whether a node is an intruder or not.

Disadvantage: It relies on reliable reference data, which is not always easy to get in underwater environments.

- Hybrid Detection

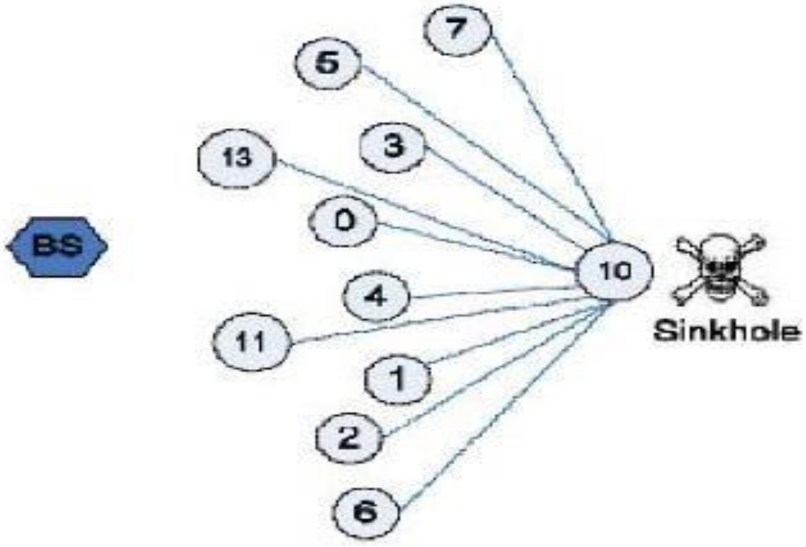
This combines techniques like anomaly and signature-based detections to achieve high level accuracy.

Advantage: It can identify known attack patterns and new patterns as well.

- key Management Solutions.

It maintains data integrity by verifying messages between nodes using secure cryptographic processes.

Advantage: Increases security by lowering the adversary's ability to compromise communications [20]

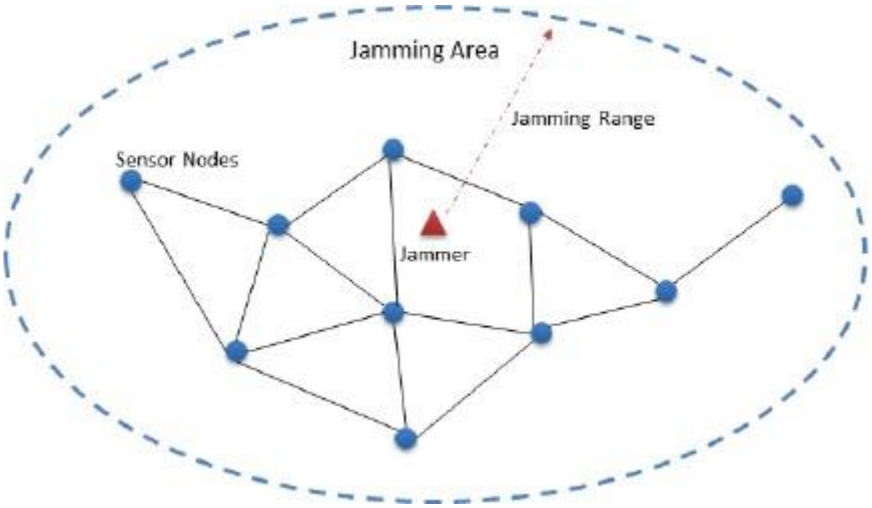


Types of Denial of Services attacks in UWSNs

Jamming attack

A jamming attack disrupts legitimate communications by injecting unwanted signals into the network channel, which captures the communication medium and prevents the exchange of data between nodes. Such an attack is very dangerous, since it does not require any special hardware to do the attack because any malicious party who has access to an open communication medium can interfere with transmissions. This type of attack is not overly expensive to implement, making it an easy option for attackers who try to cause damage at minimal cost [12].

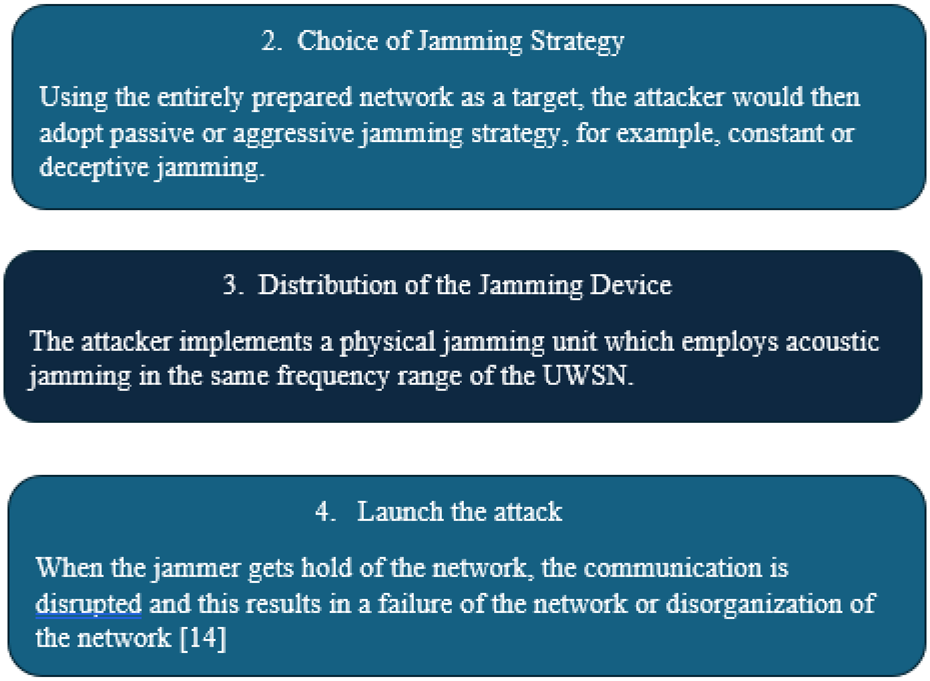
These jamming attacks can be small-scale or large-scale. Small scale jamming attacks block data from underwater research sensors and large-scale attacks disable any essential maritime defense or environmental monitoring systems [14].



How do Jamming Attacks work in UWSNs?

1. Exploration of the Network

The UWSN capabilities such as the range of the nodes, the frequency of data transmission, and the locations of nodes and access points are identified by the attacker.



2. Choice of Jamming Strategy

Using the entirely prepared network as a target, the attacker would then adopt passive or aggressive jamming strategy, for example, constant or deceptive jamming.

3. Distribution of the Jamming Device

The attacker implements a physical jamming unit which employs acoustic jamming in the same frequency range of the UWSN.

4. Launch the attack

When the jammer gets hold of the network, the communication is disrupted and this results in a failure of the network or disorganization of the network [14]

Types of jamming attacks in UWSNs

- Constant Jamming

A continuous acoustic signal is transmitted to interfere with all communications in the network. The result is a complete denial-of-service situation for all devices.

- Deceptive Jamming

An attacker generates fake sensor data to trick network nodes into accepting malicious signals as authentic. This might lead to false data collection or navigation.

- Reactive Jamming

It is activated only when the jamming device detects legitimate communication. Therefore, it is harder to detect while preserving the attacker's energy.

- Random Jamming

The jammer randomly switches between sleeping and injecting packets [12].

Countermeasures to mitigate Jamming Attacks in UWSNs

- **A learning-based power control strategy**

Introduced by Xaio in 2015 to address jamming attacks with unknown channel parameters of the attacker [12].

- **A jamming detection algorithm including an underwater jamming detection protocol**

Introduced by Misra where nodes strategically exchange discovery and acknowledgement packets [12] [15].

- **An efficient channel allocation scheme and a novel cross-layer design**

Used for cooperative communication to detect jammed nodes and utilize the spectrum efficiently [12] [16].

- Jamming Detection Systems

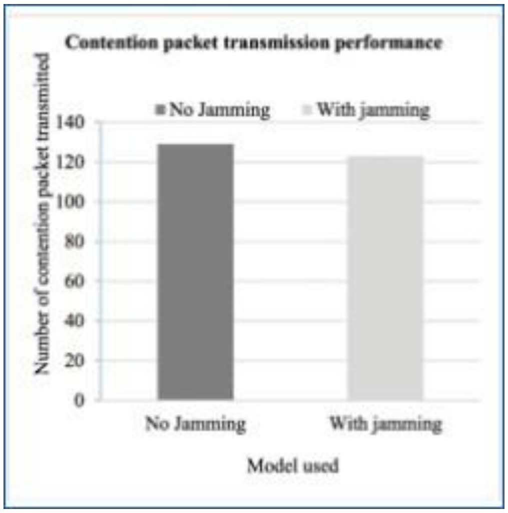
A method where an Intrusion Detection System (IDS) is used to observe the network for ongoing traffic flow and to look for traffic pattern abnormalities that may be present along the interference.

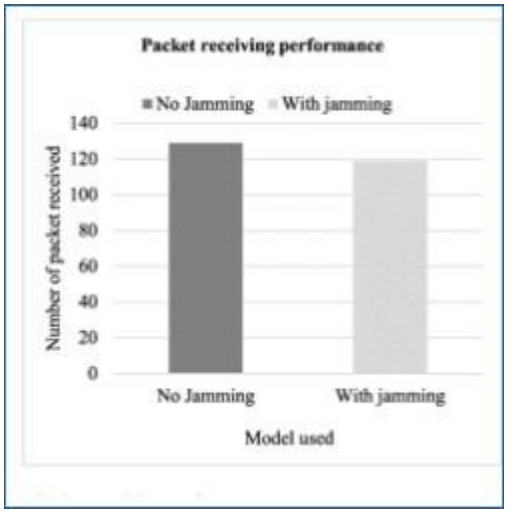
- Adaptive routing and network coding

Total jamming can be avoided if alternative paths are adopted for routing of data and even encoding of the information was used instead of realizing communication only.

- Relay-based communication

Introduce additional relay nodes to Geographical Fault Tolerance allowing for the continued flow of data range even if some of the nodes are jammed [14].





Flooding Attacks – Hello Flood

In UWSNs, flooding attacks can disturb the smooth operations of the network and the data within any nodes by continuously flooding them with data packets. A flooder, or an attacker, pretends like a normal node and sends out many hello packets to closer nodes, making them categorize the attacker as a legitimate neighbor [21].

Features of Flooding Attacks

Network Congestion: The increased volume of traffic created, causes blockage within the network and interferes with the ratio of successful packet deliveries.

Resource Drain: Legitimate nodes waste energy by trying to react to fake threatening neighbors, which will reduce their lifespan.

Disruption of Communication: One of the other effects flooding may cause is countless distributions, which sabotages normal patterns of communications and interrupts nodes' ability to send or receive any information [21].

Countermeasures against Flooding attacks in UWSNs

- Authentication Schemes

The hello-based schemes require strong authentication mechanisms to enable only legit nodes which are always allowed into the network. This includes technologies like digital signatures and cryptographic mechanisms.

- Rate limiting

Creates a limit on how many hello packets can send from each node, so the flood is less likely to happen.

- Neighborhood verification

Before a node trusts information from its neighbors, the nodes need to first validate their neighbors through multiple communication rounds. It can help to prevent nodes from accepting hello packets from potential malicious sources.

- Adaptive Routing Protocols

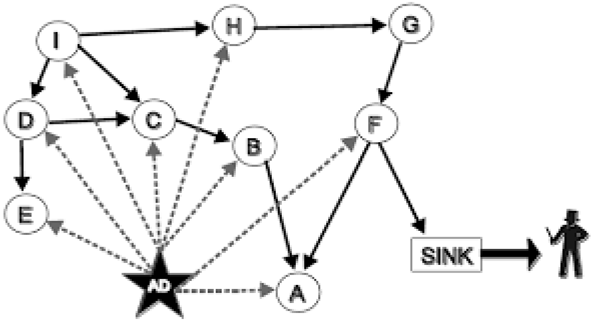
Uses routing protocols that are dynamic and adjust to flooding attacks by detecting abnormal (packets) traffic patterns, which go out of the route.

- Energy-Aware Protocols

If a network uses energy aware protocols, those policies will do battery conservation by reducing the number of unnecessary transmissions. That will reduce the flooding attacks on the network.

- IDS (Intrusion Detection Systems)

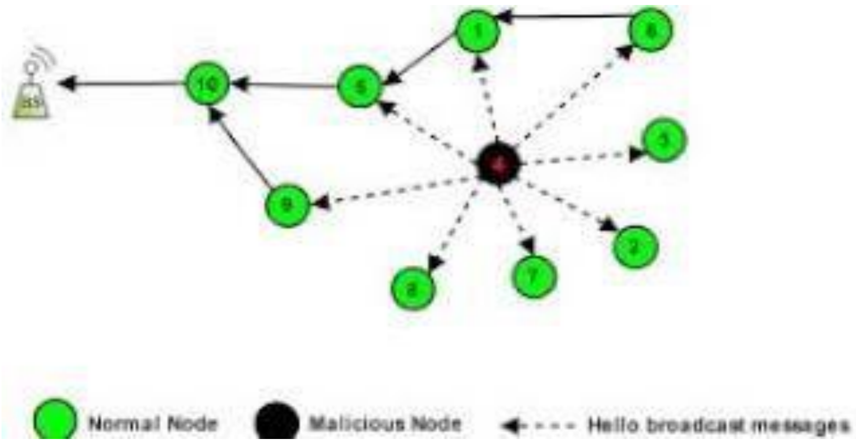
Use IDS to monitor traffic patterns and to identify anomalies that are consistent with flooding attacks in real time [21].



Spoofing Attacks

Spoofing attacks are a prominent threat in UWSNs because a lot of information is exchangeable via wireless transmissions. In this attack, Mac addresses are captured through network monitoring by attackers and then they use the fake address to impersonate the legitimate nodes [22].

A different type of spoofing attack is acknowledgement spoofing in which a malicious node listens to the communications of neighbor nodes and transmits false link-layer acknowledgements. This brings confusion within the network that could lead to packet loss and disruption of the network which is a form of DoS attack [12].



Countermeasures against Spoofing Attacks in UWSNs

- Asymmetric-key cryptography-based authentication

Utilizes encryption to validate identities but this approach might require many resources and energy for UWSN nodes.

- Detection based on localization

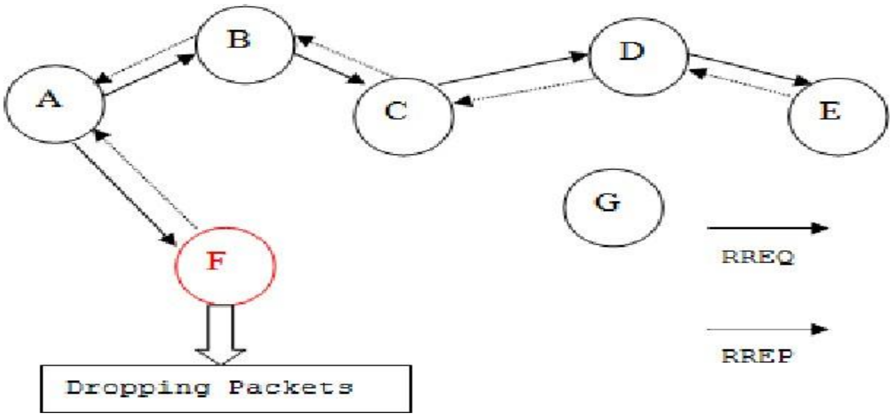
Identifies attack nodes' locations using signal-based localization and then further investigate it [22].

- Dynamic key distribution

Uses of dynamic keys which will reduce the impact when the keys are compromised.

Blackhole Attacks

Black hole attacks remain one of the main threats to UWSNs. In here, one malicious node impersonates the destination node or forges the Route Reply messages by tricking the source into sending data through it. Then the attacker discards the packets instead of forwarding them to their intended destination, resulting in a DoS attack as the communication becomes disrupted and the network performance is compromised. Since UWSNs communicate across open water and due to limited resources, these attacks affect data transmission immensely [12] [23].



General countermeasures to mitigate the overall Attacks in UWSNs

- Improving Existing Algorithms

Routing Algorithms: Improved routing algorithms are able to avoid attacks such as Wormhole, sinkhole and Sybil and also guarantee secure data delivery [12].

Localization Algorithms: Highly accurate localization algorithms maximize the chances of capturing data from the relevant and intended area.

Data Aggregation Algorithms: Strong aggregation helps in lowering the communication costs, promoting energy efficiency and protecting data from malicious modifications.

- Using Cryptographic Tools

Encryption: Safeguard the confidentiality of the data in transit through symmetric key encryption between the nodes and the base station.

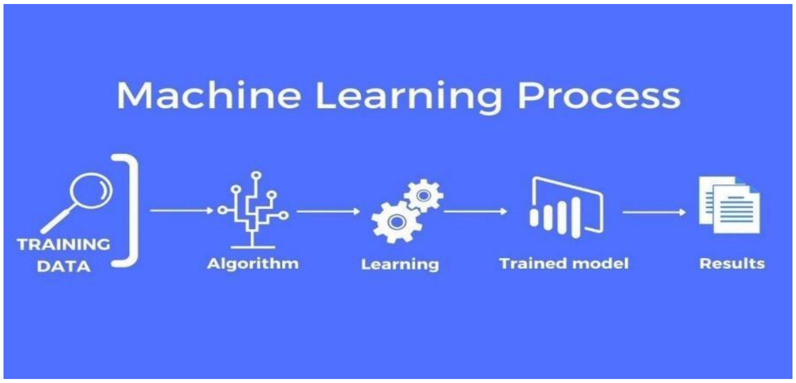
Digital Signatures: It helps in proving the authenticity of the data by making it easier to identify spoofing attacks.

Key Management Schemes: Ensures that secure distribution of keys is achieved without much computational cost [12].

- Applying Machine Learning Models

Intrusion Detection: It is a construction that makes use of machine learning and attempts to identify malicious actions by analyzing traffic patterns (Ex: DoS attack detection).

Malicious Node Detection: Methods such as Support Vector Machines help track down and isolate compromised nodes based on their actions [12].



Future Research Directions for UWSN Security

After analyzing the above research findings, the following provides suggestions for future research on the security of UWSNs.

- **Developing a Standardized Security Architecture for UWSNs**

In current situations, most of the security measures for UWSNs are experimental and address only a single threat or a group of threats due to limitations such as limited bandwidth, complex latency and underwater device resources constraints.

Therefore, a more robust security architecture that would include protocols and policies for multi-layered security is necessary to guide the design of future UWSNs [12].

Example findings

Bagali and Sundaraguru introduced a model for reactive jamming detection that shows significant improvement over previous models [12] [20].

SenseVault framework proposed by Xu and Liu with contributions such as adapting to dynamic environments, authentication and cryptography [12] .

- **Improving energy sources and consumption**

Energy shortage and high energy consumption are major issues in UWSNs as they directly relate to the energy required for securing UWSNs. Further development is necessary to explore better energy sources, energy-efficient and low-computation overhead security measures [12]. This will broaden the scope of effective security with low risks.

Further research should focus on energy harvesting techniques such as accumulating energy from underwater currents or temperature gradients to extend the lifetime of UWSNs and enable more robust security.

- **Conducting more physical Experimentations**

Most research works that highlight security mechanisms are evaluated by simulations, which have predefined constraints. Simulations provide a cost-effective and time-effective way to test new concepts and are valuable for experimental research. However, due to the unpredictable nature of the underwater environment, simulation software does not capture accurate behaviors that result in inaccuracies [12].

More physical experiments can be done to evaluate the effectiveness of UWSN security.

❖ **Examine Lightweight and Energy-Efficient Security Protocols**

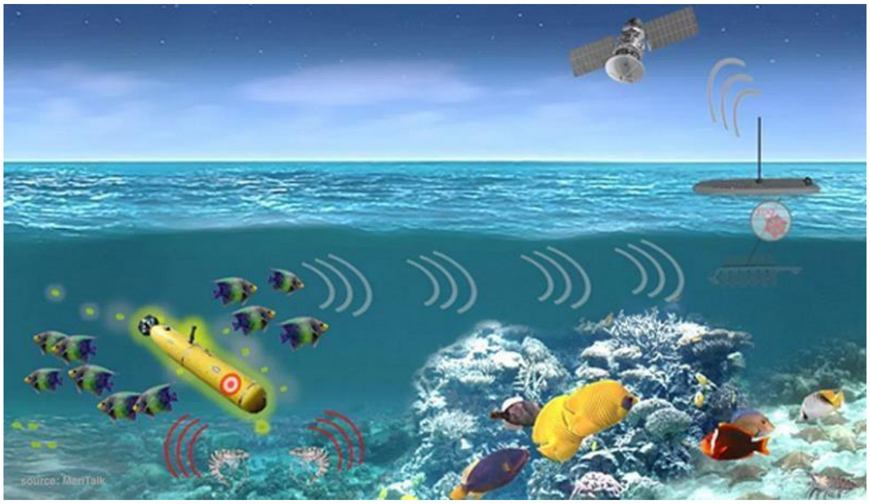
Researchers in UWSNs should consider developing security measures that are energy-efficient and less complex due to energy constraints that UWSNs have.

This extends to the development of encryption algorithms, key management systems, and authentication techniques suitable for underwater applications.

❖ **Focus on Denial-of-Service attacks**

Most research regarding UWSN security is focused on DoS threats, highlighting that it is the most dangerous threat to these networks. This focus arises due to the high energy consumption of the sensor nodes and the dependence on unreliable and range unstable acoustic communication, which aggravates the DoS effects.

It is evident that research on DoS attack countermeasures is critical for UWSN security.



source: MeriTalk

Conclusion

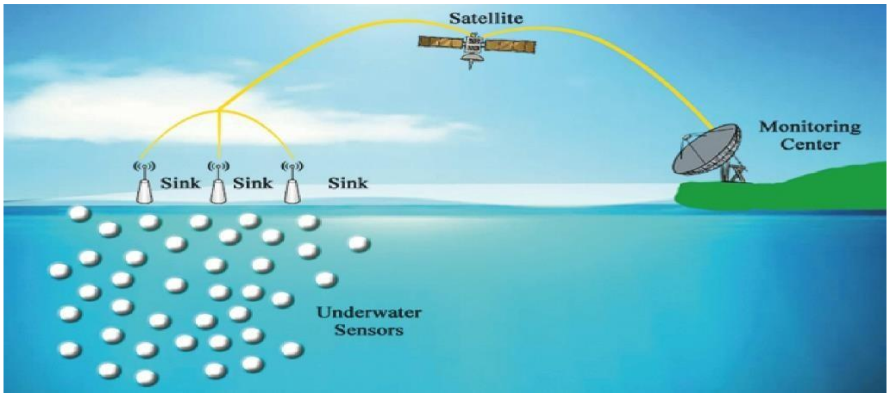
This report highlights the concept of IoUT technology, its applications, and the security challenges presented by it, with a specified focus on UWSNs. It initiates by presenting the concept of IoUT,a new network structure of underwater-connected devices along with its importance for areas like environmental monitoring, underwater exploration, and disaster prevention. The report then outlines the characteristics of UWSNs and how these attributes directly implicate the security of the network.

A major finding of the report is the exploration of various attacks that may be launched against integrity, availability, and confidentiality in UWSNs.

Routing attacks such as Wormhole, Sybil, and sinkhole, are based on weaknesses in the communication protocols to interfere with the flow of data with the intent to compromise the functionality of the network. The report also explains how these attacks operate and the consequences. Besides routing attacks, it also explores DoS, such as jamming, flooding, and spoofing, and shows how these could overwhelm network resources and disable communication.

Among the contributions, the report goes on to present some of the **future research directions** that could be pursued in enhancing UWSNs security and even went further to propose the development of a standardized security architecture as a way of reforming the shortcomings of the ad-hoc approach.

Furthermore, innovative energy sources and energy-efficient security protocols are under study in order to overcome the energy constraint of UWSN nodes. Physical experimentations to validate the proposed security mechanisms in realistic conditions and focus on developing robust countermeasures against DoS attacks are pointed out in this report.



References

[1] P. K. C. S. S. C. Binaya Kumar Mishra, "Water Security," *Water Security in a Changing Environment: Concept, Challenges and Solutions,* no. February 2021, p. 21, 2021.

[2] M. T. A. S. A.-M. K. Sunil Sharma, "Cybersecurity in water," *Overcoming vulnerabilities to build a vigilant, resilient and secure critical water infrastructure,* no. 08 July, 2023, p. 12, 2023.

[3] S. FelembanE, *Underwater Sensor Network Applications: A Comprehensive Survey.,* no. International Journal of Distributed Sensor Networks , pp. 1-14, 2021.

[4] " Internet of Things Global Standards Initiative," ITU-T IoT-GSI, [Online]. Available: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. [Accessed 29 september 2024].

[5] C. Sharma, "Correcting the IoT History," Chetan sharma consulting , [Online]. Available: https://www.chetansharma.com/correcting-the-iot-history/. [Accessed 29 september 2024].

[6] M. C. Domingo, "Journal of Network and Computer Applications," *An overview of the internet of underwater things,* vol. 35, no. 6, pp. 1879-1890, November 2012.

[7] Y.-S. L. G.-D. W. C.-J. H. Chien-Chi Kao, "MDPI," *A Comprehensive Study on the Internet of Underwater Things: Applications, Challenges, and Channel Models †,* vol. 17, no. 7, 2017.

[8] D. N. R. M. a. M. A. A. S. EL-Rabaie1, *Underwater Wireless Sensor Networks (UWSN), Architecture, Routing Protocols, Simulation and Modeling Tools, Localization, Security Issues and Some Novel Trends,* August 2015.

[9] N. G. A. B. L. K. A. A. A. A. S. Monika Chaughary, "IEEE," *Underwater Wireless Sensor Networks: Enabling Technologies for Node Deployment and Data Collection Challenges,* vol. 10, no. 4, pp. 3500 - 3524, 15 February 2023.

[10] T. DasA, "2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)," *Secure communication in mobile underwater wireless sensor networks,* August 10-13, 2015.

[11] L. D. G. S. S. W. S. W. Guang Yang, "Procedia Computer Science," *Challenges and Security Issues in Underwater Wireless Sensor Networks,* pp. 147:210-216, 2019.

[12] T. D. S. B. H. Aliyu Gana Yisa, " Transactions on Emerging Telecommunications Technologies," *Security Challenges of Internet of Underwater Things: A Systematic Literature Review,* p. 18, March 2021.

[13] D. N. R. M. a. M. A. A. S. EL-Rabaie, "Faculty of Electronic Engineering, Dept. of Communication Engineering, 32952 Menouf, EGYPT," *Underwater Wireless Sensor Networks (UWSN), Architecture, Routing Protocols, Simulation and Modeling Tools, Localization, Security Issues and Some Novel Trends,* p. 22.

[14] "Wormhole Attack in Wireless Sensor Networks," geek for geeks, 04 May 2023. [Online]. Available: https://www.geeksforgeeks.org/wormhole-attack-in-wireless-sensor-networks/. [Accessed 16 October 2024].

[15] W. S. Y. M. R. Shams Qazi, "Securing DSR against wormhole attacks in multirate ad hoc networks," *Journal of Network and Computer Applications,* vol. 36, no. 2, pp. 582-592, March 2013.

[16] "What Is a Sybil Attack?," Chainlink, 30 August 2024. [Online]. Available: https://chain.link/education-hub/sybil-attack. [Accessed 17 October 2024].

[17] "Sinkhole Attack in Wireless Sensor Networks," geeks for geeks, 17 March 2023. [Online]. Available: https://www.geeksforgeeks.org/sinkhole-attack-in-wireless-sensor-networks/. [Accessed 17 October 2024].

[18] "Jamming Attacks," SEON, [Online]. Available: https://seon.io/resources/dictionary/jamming-attacks/. [Accessed 12 October 2024].

[19] S. D. M. K. A. V. M. O. S. Misra, "Jamming in underwater sensor networks: detection and mitigation," *IET Communications,* vol. 6, no. 14, p. 2178–2188, 2012.

[20] R. S. Sheetal Bagali, "Maximize resource utilization based channel access model with presence of reactive jammer for underwater wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE) ,* vol. 10, no. 3, p. 3284~3394 , June 2020.

[21] R. K. V. B. Kapil Mangla, "Analysis of Flooding Attacks on Wireless Sensor," *IJLTEMAS,* vol. 3, no. 5, May 2014.

[22] C. R. Prasuna Kotturu, "SPOOFING ATTACK - A THREAT IN WIRELESS SENSOR NETWORKS," *International Journal of Innovative Research and Practices,* vol. 3, no. 3, March 2015.

[23] D. P. Umashankar Ghugar, "A Study on Black Hole Attack in Wireless Sensor Networks," *International Journal of Advance Computing Techniqueand Applications (IJACTA),* vol. 5, no. 1, 2017 January- June.