Lightweight Multi-factor Authentication for Underwater Wireless Sensor Networks

Ahmed Al Guqhaiman*†, Oluwatobi Akanbi*, Amer Aljaedi‡, C. Edward Chow*
* *Department of Computer Science, University of Colorado Colorado Springs, Colorado Springs, CO 80918, USA*
†*Department of Computer Networks and Communications, King Faisal University, Hofuf 31982, Saudi Arabia*
‡*College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia*
{*aalguqha,oakanbi,cchow*}*@uccs.edu, aaljaedi@ut.edu.sa*

***Abstract*—Underwater Wireless Sensor Networks (UWSNs) are liable to malicious attacks due to limited bandwidth, limited power, high propagation delay, path loss, and variable speed. The major differences between UWSNs and Terrestrial Wireless Sensor Networks (TWSNs) necessitate a new mechanism to secure UWSNs. The existing Media Access Control (MAC) and routing protocols have addressed the network performance of UWSNs, but are vulnerable to several attacks. The secure MAC and routing protocols must exist to detect Sybil, Blackhole, Wormhole, Hello Flooding, Acknowledgment Spoofing, Selective Forwarding, Sinkhole, and Exhaustion attacks. These attacks can disrupt or disable the network connection. Hence, these attacks can degrade the network performance and total loss can be catastrophic in some applications, like monitoring oil/gas spills. Several researchers have studied the security of UWSNs, but most of the works detect malicious attacks solely based on a certain predefined threshold. It is not optimal to detect malicious attacks after the threshold value is met. In this paper, we propose a multi-factor authentication model that is based on zero-knowledge proof to detect malicious activities and secure UWSNs from several attacks.**

***Keywords*-Underwater Wireless Sensor Networks, Terrestrial Wireless Sensor Networks , Security, Malicious Attacks**

I. Introduction

Recently, UWSNs have received rapidly growing interest from the research community because they allow underwater nodes and sinks at different depths to communicate together. UWSNs play a crucial role by monitoring several applications, such as environmental monitoring, disaster prevention, pollution monitoring, and oil/gas spills detection. UWSNs face many challenges, including limited bandwidth, high transmission loss, long propagation delay, multipath effect, doppler spread, and other environmental weaknesses compared to TWSNs [1]–[3]. The above characteristics make communication less reliable and the network less energy efficient. In addition, improving these significant factors will prolong the network lifetime, secure underwater communication, and enhance network performance in several metrics. Hence, securing packets using the TWSN techniques is not efficient for the UWSN environment. Therefore, a new technique must be developed based on UWSNs' characteristics.

UWSNs consist of a set of sensor nodes, gateway nodes, and buoys (also known as sink nodes). Sensor nodes collect information about the status of an environment. All collected data is transmitted to the gateway node. The gateway node has higher resources in terms of processing, memory, power, and storage. The gateway node aggregates the incoming data and transmits the data to the buoy at the surface level.

UWSNs are different from TWSNs in many aspects. The available bandwidth can start from less than 1 kHz up to 100 kHz. The bandwidth depends on the distance between nodes and signal frequency. Since the available bandwidth is very limited, the speed of sound is extremely slow (1,500 meters/sec) compared to the speed of light (300,000,000 meters/sec). The variables of propagation delay and wave reflection can cause multipath effects. Transmission loss may occur because of geometric spreading and attenuation. High transmission loss may occur due to the distance between nodes and signal frequency. Acoustic waves can suffer from man-made noise (e.g., machinery noise and shipping activities) or natural noise (e.g., currents, seismic, and biological activities). Noise can cause collisions of the ongoing packets, which ultimately degrade underwater communication. Doppler spread may occur due to mobile nodes and communication range. Table I shows the major differences between TWSNs and UWSNs. This new environment introduces challenges and issues that must be addressed while designing an appropriate protocol for the UWSN environment.

All existing UWSNs consist of limited resource nodes, which encourages researchers to find an ideal approach that supports both powerful and constrained nodes. A higher level of security and low overhead are needed. The purpose of this study is to meet the requirements of real-time applications, such as the oil/gas industry. To implement UWSNs in the oil/gas industry, we must be able to transmit packets with minimal delay and energy consumption, while maximizing the Packet Delivery Ratio (PDR). In addition to network performance requirements, critical applications require security services. Underwater communication can be compromised in the absence of protection from malicious attacks. These requirements are necessary to avoid a high total loss.

The content of this paper is structured as follows: Section

978-1-7281-7624-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CSCI51800.2020.00039

Table I: Characteristics of TWSNs vs. UASNs [4, 5]

Parameters	TWSNs	UWSNs
Common Communication Modality	Radio waves	Acoustic waves
Propagation Speed	300,000,000 m/s	1,500 m/s
Transmission Range	10 m - 100 m	Up to 10 Km
Frequency	908 - 928 MHz	10 Hz - 100 KHz
Mobility of Nodes	Application-based	Generally mobile
Reliability of Links	Application-based	Low
Stability of Links	Stable	Unstable
Localization	GPS supportive	GPS non-supportive
Node Density	Dense	Generally sparse
Energy Consumption	Low	High
BER	Moderate	High
Path Loss	Low	High
Noise	Less impact	High impact
Common Data Flow Mode	Full Duplex	Half Duplex
Common Flow and Error Control Protocol	Selective Repeat ARQ or Go-Back-N ARQ	Stop-and-Wait ARQ
Memory	Have less capacity	Require large capacity
Cost	Cheap	Expensive

II presents the security challenges of UWSNs, including security requirements, secure communication, and secure protocols. Section III briefly describes some related work. Section IV describes our proposed multi-factor authentication. Section V concludes the paper and recommends future research.

II. UWSN Security

Since most of the existing research papers focus on developing new methods to enhance the communication in UWSNs, the UWSNs' environments are vulnerable to several attacks from the physical layer up to the application layer. An adversary can send fake packets or advertise invalid information to nodes by sending a large number of packets to reduce system availability. External attacks are more likely in UWSNs' environment as nodes in UWSNs exist in open space. Internal attacks may occur as well, but the probability of an internal attack is lower as we assume nodes are fixed and can only communicate with predefined trusted nodes.

The locations of sensors and sinks are fixed after deployment. Sensor nodes are responsible to collect data and forward it to the gateway. The gateway then aggregates the data and forwards it to the buoy. To detect a malicious attack, several metrics must be considered, such as Hop Count (HC), available throughput, and memory space. Using these metrics, sensor and sink nodes should be able to detect several attacks.

Many papers have studied the security of UWSNs by utilizing expensive cryptographic approaches similar to those used in conventional networks. These cryptographic approaches are not appropriate for UWSNs as they require high resources. UWSNs are more vulnerable to severe attacks due to their limited resources. Malicious attacks can be active attacks or passive attacks. Active attacks occur when an adversary tries to change, inject, delete, or destroy transmitted data [6]. In contrast, passive attacks occur when an adversary observes the ongoing communication and copies the ongoing packets to use them for malicious activities. These types of attacks are harder to detect. Considering the UWSNs' characteristics, many algorithms initially designed for TWSNs cannot be implemented in UWSNs. Therefore, new security mechanisms must be developed, bearing in mind the UWSNs' limitations.

A. Security Requirements

UWSNs require the same essential security services as TWSNs, including confidentiality, integrity, availability, authentication, freshness, and non-repudiation [7]–[10].

1) Confidentiality (C). Confidentiality guarantees that exchanging packets between valid nodes cannot be accessed by an unauthorized party. Military applications require secrecy for marine surveillance.

2) Integrity (I). Integrity assures that packets have not been changed by an adversary during transmission. Integrity is required to monitor water quality.

3) Availability (A). Availability ensures that data is available to an authorized party when it is needed. Denial of Service (DoS) attack will cause a high loss in case of natural disasters, such as tsunami and flood.

4) Authenticity. Incoming packets must be authenticated to make sure the sent packets came from a valid neighbor node. Once a packet has been authenticated, it can be exchanged in a secure manner.

5) Freshness. Freshness requires that data is new and ensures that no old messages have been replayed. In encryption, the key freshness refers to the key that changes over time to defend against a replay attack.

6) Non-repudiation. Non-repudiation means that a node cannot deny that it did not perform specific actions, including sending or receiving data. Non-repudiation can be achieved via the digital signature.

B. Secure Communication

In general, a malicious attack targets UWSNs in two ways: either attacking the nodes or attacking the communication protocols [2]. A successful attack on the nodes can cause much more physical damage to the network than attacking the communication protocol. However, due to the large distance between nodes, it is difficult to destroy a set of nodes concurrently. Hence, the first type of attack does not cause high damage unless the compromised node is a sink node. On the other hand, attacking the communication protocol of UWSNs is more common. A successful attack

on the communication protocol results in a useless network as an adversary can destroy the entire network. Therefore, in this paper, we focus on securing the MAC and routing protocols from well-known attacks.

Currently, there is very limited research on protection measures for UWSNs which leaves UWSNs vulnerable. Abnormal activity is an efficient way to detect malicious attacks. More specifically, the focus of this paper is to detect malicious attacks and protect packets at the MAC and network layers from well-known attacks.

C. Secure Protocols

Most existing MAC and routing protocols for UWSNs have been designed without considering the security aspects [11]. Therefore, the entire network can be unavailable because of malicious attacks, such as Sybil, Blackhole, Wormhole, Hello Flooding, Acknowledgment, Selective Forwarding, Sinkhole, and Exhaustion [7]–[10].

1) Sybil Attack. Sybil attack is one of the most common attacks in the network layer. Figure 1 illustrates an example of a Sybil attack. First, adversaries fake new identities or steal existing identities and claim to be a trusted node. The malicious node then sends incorrect information to misdirect the data through a malicious route. Once a trusted node accepts the incorrect information and updates its routing table, an adversary can control the packets that pass through nodes under the attacker's control. It is highly possible that packets will experience longer delay and/or high drop rate. Several works resolved the problem by using the physical location of nodes or encryption as a security measure. The encryption methods require high resources in terms of storage, power, and computing capability, which is not available in UWSNs. Li et al. [12] propose a technique where they take advantage of network information to detect Sybil attacks. In Fig. 1, when node A wants to send packets to F, it broadcasts its request. Based on the network topology, node A knows that it cannot communicate with node F directly. Therefore, packets must pass through node D to reach F. A malicious node will respond to node A claiming to be node F. Since node F is not a listed neighbor, node A rejects this response and labels the malicious node as a Sybil node. If a malicious node claims to be a neighbor node, node A needs to check the responses from its neighbor and any duplicate responses where one of these responses is a Sybil. Next, node A compares the parameters and based on the network information, it can detect the Sybil node [13].

2) Blackhole Attack. Blackhole attack is an attack where a malicious node impersonates the destination or advertises the shortest path to a valid node [14]. By choosing the malicious node as a relay, the network degrades because the attacker drops incoming packets. Multipath routing and location authentication can be used to defend against this attack.

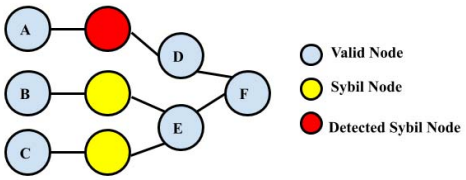

Figure 1: Sybil Attack

3) Wormhole Attack. Wormhole attack occurs when an attacker presents a path through two malicious nodes with better resources than the existing path [7]. Figure 2 represents an example of a Wormhole attack. This attack can disrupt or disable network connectivity by changing the network map of the valid topology. From a valid node's view, the advertised path to the destination appears to be shorter which may lead valid nodes to conclude that the Wormhole tunnel is a better route. The choice of the Wormhole tunnel to forward packets will help the attacker to initiate a replay attack. A replay attack occurs when an adversary has valid information and replays this information to another part of the network. One way to prevent this attack is by using geographical information. When a sensor node receives packets from the untrusted node, it considers these packets to be malicious packets.

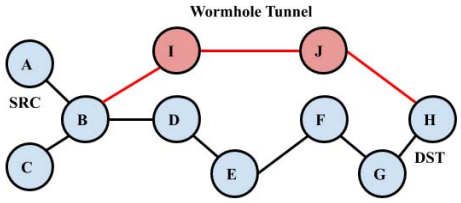

Figure 2: Wormhole Attack

4) Hello Flooding Attack. Hello Flooding attack occurs when an attacker broadcasts the hello packet to neighbors where valid neighbors believe this packet is coming from a valid neighbor [7]. Multi-factor authentication helps to defend against this type of attack. The issue here is that multi-factor authentication requires high memory space and high computation, which are not available in UWSNs.

5) Acknowledgment Spoofing Attack. When a packet is sent through the network, an attacker can have a copy of this packet and use it to spoof the link layer [7]. The attackers may be able to spoof the link layer by trying to update existing links to links under the attacker's control. This attack results in high Bit Error Rate (BER) and unreliable connection. To defend against this type of attack, all transmission packets must be encrypted.

6) Selective Forwarding Attack. In this attack, an attacker compromises one of the valid nodes. When neighbors transmit packets, an adversary drops specific packets [7]. This

results in degrading the network performance by requiring the source or sink node to retransmit lost packets. Multipath routing and location authentication can resolve this attack. Authenticating routing information is another way to defend against this attack.

7) Sinkhole Attack. An attacker advertises false routing information to attract neighbors to forward packets through this route [7]. By forwarding packets through an untrusted routing path, the attacker can thereafter conduct selective forwarding attack. Clearly, using untrusted routing information results in degrading the network performance. Similar to selective forwarding, authenticating routing information and utilizing multipath routing can protect UWSNs from this type of attack.

8) Exhaustion Attack. A malicious node keeps sending useless packets to neighbors to exhaust their power [8]. When a valid node processes these packets, it results in lower system availability. Setting firewall policies where a node drops all packets coming from unknown nodes can defend the network against this type of attack. In this case, valid nodes will not process packets that come from unknown nodes. This defense mechanism is most effective when nodes are fixed, and valid nodes are known.

The discussed malicious attacks target more than one layer. If we implement a security service for each layer, then the power of nodes will exhaust more quickly. Cong et al. [15] discuss that layered security mechanisms cannot defend against cross-layer attacks. Cross-layer security can satisfy these requirements but this is not the most effective approach [15]. Therefore, we need to design security mechanisms that can be used to defend more than one layer while minimizing energy consumption.

In general, defenses in TWSNs cannot be implemented in UWSNs. We must consider the characteristics of UWSNs and make changes based on these characteristics. Each layer is susceptible to several attacks and system security can be improved by implementing the following defense techniques [16]. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are common ways to protect the physical layer from jamming attacks. To protect the data link layer, redundancy and error correction are common ways to work with corrupted or lost packets. The network layer can reroute packets to the near-optimal path to avoid packet loss. The transport layer can deploy a handshaking technique to detect malicious activity. The attacks discussed previously can affect different layers on the Transmission Control Protocol/Internet Protocol (TCP/IP) model. Table II below shows classification of attacks, which attack affects which layers, and common defenses.

Table II: Summary of Attacks [10, 17, 18]

Type of Attack	Classification of Attacks	TCP/IP Layer	Common Countermeasures
Sybil	C, I, A	2, 3, 5	Secure positioning, encryption, authentication, RSSI
Blackhole	C, I, A	3	Multipath routing, location authentication, monitoring, IDS
Wormhole	C, I, A	3	Geographical information, DoA, monitoring, authenticate neighbors
Hello Flooding	A	2, 3	Multi-factor authentication, monitoring, geographic routing
Acknowledgment Spoofing	I, A	2	Encryption, authentication
Selective Forwarding	C, I, A	3	Multipath routing, location authentication, routing information authentication, reputation and trust
Sinkhole	C, I, A	3	Routing information authentication, multipath routing, monitoring
Exhaustion	A	2, 3, 5	Firewall policies, limit number of retransmissions, monitoring

2: Data Link, 3: Network, 5: Application

III. Related Work

Several protocols and security mechanisms have been proposed in UWSNs. In this section, we present some related methods to achieve efficient and secure communication. Most of the existing protocols have been developed without considering security aspects. In order to ensure security, the network must detect malicious attacks as soon as abnormal activity exists. Without proper security mechanisms to protect UWSNs, several attacks will degrade the network performance or disrupt the entire system.

To detect intrusion, TWSNs have used statistical analysis [9]. This strategy can detect external routing attacks only. Based on the routing information, this common mechanism can detect abnormal activity using statistical analysis. It is not an effective approach to detect internal attacks and cannot be applied in UWSNs. Therefore, another work proposes a prevention mechanism to secure routing from external attacks [2]. These approaches can detect several attacks, such as Sybil, Selective Forwarding, Blackhole, Greyhole, and Sinkhole attacks. However, the issue with these works is that neither of them can detect internal attacks. Therefore, Ahmed et al. [9] detect malicious activity based on the HC metric. When a sensor node receives packets from a malicious node, the sensor node can use the HC to detect an attacker. This technique works when a malicious node advertises a lower HC than the one stored in a valid node but may fail to detect an attacker that advertises the same HC. A malicious attacker may match with one metric, but not more than one. The probability of a malicious attacker

matching the expected behavior based on more than one metric is very low. Therefore, multiple metrics should be considered as well to detect malicious behavior.

Ateniese et. al [8] investigated a Security Framework for Underwater acoustic sensor Networks (SecFUN). This employs the building block Galois Counter Mode (GCM) for authentication and encryption purposes with 128-bit block cipher, such as Advanced Encryption Standard (AES). This work also proposed a Security version of the Channel Aware Routing Protocol known as Se-CARP. Each node has two keys, a group key shared with several nodes and a unique key shared with the sink node. The shared group key is used to authenticate and encrypt incoming packets to look for the best relay among a node's neighbors. In contrast, the unique key is used to authenticate and encrypt all packets exchanged with the sink. Even though the use of particular features of GCM makes AES encryption simple, it may require high resources which are not available in UWSNs.

Han et. al [2] proposed an Attack-Resistant Trust Model based on multidimensional trust Metrics (ARTMM), which trusts incoming packets based on a node's reputation. The reputation model considers the UWSNs characteristics and node mobility. This trust model has three types of trust metrics, which are link trust, node trust, and data trust. The trust values of these metrics are based on link quality, link utilization, and node honesty. Each node must maintain these values, which requires a high level of computation to evaluate incoming packets. This may consequently result in high end-to-end delay and overhead.

IV. Proposed Detection and Mitigation Approach

UWSNs are more prone to internal and external attacks compared to TWSNs as nodes are deployed in open unprotected space. Therefore, nodes underwater may fail to sense an environment or to communicate with other nodes due to attacks or system failure [16]. When a compromised node exists within the network, this node behaves maliciously by dropping packets, forwarding packets to unknown nodes, or broadcasting a large amount of data. Underwater nodes that overhear these transmissions should be able to report the malicious activity to their assigned sink and block themselves from accepting packets from the malicious node [13].

Existing utility functions rely on HC and remaining energy. These schemes work best when the connection is reliable and the nodes have sufficient resources similar to nodes in TWSNs. Relying solely on these metrics may not be enough to detect malicious activities. Therefore, underwater nodes need additional information to evaluate incoming packets. In a conventional network, each node maintains many values, which can be expensive with limited resources. Thus, we propose multi-factor authentication that is based on zero-knowledge proof by updating the header information to include an Identifier based on the MAC address (IMAC), Direction of Arrival (DoA), and HC to validate incoming packets. In this way, all underwater nodes can validate incoming packets without further communication to the sink, accurate time synchronization, or accurate localization.

In our approach, each node overhears ongoing packets within its Transmission Range (TR) and extracts the header of these packets. To authenticate incoming packets, each node must compare header information with stored information about its neighbors within TR. If any of these metrics do not match with the stored information, the valid node labels incoming packets as malicious and then generates an alert to its neighbors and isolates itself. This technique does not require nodes to perform high computation. Our approach is broken down into monitoring phase, and detection and mitigation phase. In monitoring phase, each node overhears neighbors' communication to evaluate incoming packets. Once a node detects any packet within TR, the detection and mitigation phase assesses the packet and alerts neighboring nodes and isolates the malicious node.

The monitoring phase is responsible to extract IMAC, Angle of Arrival (AoA), and HC information from packets' headers into the monitoring report. To identify multiple requests that come from nodes within TR, we need to assign each incoming packet a unique Request Identifier (RID). Consequently, the monitoring report contains the following four fields: RID, IMAC, AoA, and HC. We assume that the network load is not high, so a node may receive up to 255 packets. MAC address is a unique identifier address that has been assigned to each Network Interface Card (NIC) so that we can distinguish between nodes within the same network. Several attacks can use legitimate MAC addresses to disrupt underwater communication. Therefore, an identifier has been used to produce an eight-bit value to avoid cloning legitimate MAC addresses of nodes. The IMAC value is assigned to each node so that we can determine trusted nodes. Several techniques can be used to measure DoA, such as Time of Arrival (ToA), Time Distance of Arrival (TDoA), Received Signal Strength (RSS), or AoA [7, 19, 20]. The ToA and TDoA cannot be used in UWSNs as the propagation delay varies. Due to a variance in propagation delay, it is difficult to detect malicious activities with a high accuracy. The RSS also varies due to noise, multipath, doppler shift, and obstacles. Thus, RSS cannot provide high accuracy, which leads to poor detection. Therefore, we choose AoA to measure the DoA as this cannot be manipulated. The value of AoA can be between 0 to 360 degrees. We assume that the network size can be up to 20 nodes, so, in the worst-case scenario, the maximum HC can be the number of network size minus one. Table III describes the meaning of all symbols that have been used in proposed algorithms. The procedures of monitoring UWSNs is summarized in Algorithm 1.

In contrast to the monitoring phase, the detection and mitigation phase is responsible to protect UWSNs from

Table III: Reference Table

Symbol	Description
Node_i	represents the values of [IMAC, AoA, HC]$_i$ from a source node where *i* refers to $\{1, 2, ...n\}$.
Pkt	represents incoming packets with a set of header information for authentication purposes.
M_r	represents monitoring report.
IMAC_i	represents IMAC of incoming packets where i refers to the Node_i.
IMAC_{si}	represents the stored IMAC of neighbor within TR where *i* refers to a neighbor number.
AoA_i	represents the AoA of incoming packets where *i* refers to the Node_i.
AoA_{si}	represents the stored AoA of neighbor within TR where *i* refers to a neighbor number.
HC_i	represents the HC of incoming packets where *i* refers the Node_i.
HC_{si}	represents the stored HC of neighbor within TR where *i* refers to neighbor number.
A_{Pkt}	accepts incoming packets for further authentication.
R_{Pkt}	rejects incoming packets and executes the protection procedures.
Auth_{Pkt}	represents the incoming packets that have been authenticated.

Algorithm 1: Monitoring Phase

Objective: To avoid malicious activities by listening into incoming packets within TR and producing monitoring report.
Input: Node_i, Pkt
Output: M_r
Initialize: RID = 0
while *overhearing Pkt* $\in TR$ **do**
  for *Node*$_i \in$ *TR* **do**
    for *RID* $>$ *0 and* $\leq$ *255* **do**
      assign RID for each Pkt into M_r
      extract IMAC, AoA, and HC from Pkt into M_r
      RID++
    end
  end
end

malicious activities. We assume that each node securely exchanges the information of multi-factor authentication and stores it locally right after deploying nodes underwater. At this point, each node knows the topology of the network and information needed to authenticate incoming packets. Since UWSNs rely on the Stop-and-Wait protocol, we can use the request identifier to protect against flooding attacks. If a node receives multiple requests from the same neighbor prior to acknowledging the previous one it must: label incoming packets as malicious, drop incoming packets, create a firewall rule to isolate the malicious node, and broadcast an alert to neighbors about this malicious activity. The alert message should include information required for neighbor nodes to update their firewall rules. We call the above actions *protection procedures*. The *protection procedures* get executed every time that a node detects malicious activities. In order to label an incoming packet as malicious, the node must first check if the IMAC value of the incoming packet is within its neighbor list. The neighbor list includes all nodes within TR. If the incoming packet is within a node's neighbor list the node compares DoA and HC with the stored values. Following the comparison, values of DoA and HC must match the stored values to be accepted, otherwise the node must perform the *protection procedures*. On the other hand, if the incoming packet is not within a node's neighbor list, the node must apply the *protection procedures*. The procedures of detection and mitigation of malicious activities in UWSNs is summarized in Algorithm 2.

Algorithm 2: Detection and Mitigation Phase

Objective: To detect and mitigate UWSNs from malicious activities.
Input: IMAC_i, IMAC_{si}, AoA_i, AoA_{si}, HC_i, HC_{si}
Output: A_{Pkt}, R_{Pkt}, Auth_{Pkt}
while $M_r \neq \varnothing$ **do**
  for *Node*$_i \in$ *TR* **do**
    Check the $IMAC_i$, AoA_i, HC_i *from* M_r;
    if M_r *contains duplicate requests* **then**
      R_{Pkt}
    else
      A_{Pkt}
    end
    Compare the $IMAC_i$, AoA_i, HC_i *from* M_r *with* $IMAC_{si}$, AoA_{si}, HC_{si}
    if $IMAC_i = IMAC_{si}$ && $AoA_i = AoA_{si}$ && $HC_i = HC_{si}$ **then**
      $Auth_{Pkt}$
    else
      R_{Pkt}
    end
  end
end

In the random forwarding algorithm, a node randomly selects a relay to carry the packets. Since the sensor and sink nodes are fixed, the multi-factor authentication functions will be helpful to detect the attacker. For example, when an attacker broadcasts a shorter route to a destination, the legitimate node can tell that the incoming update is invalid based on the node's local knowledge. So, in this case, we can protect nodes from several attacks. Another way to prevent sensor nodes from several attacks is to restrict legitimate nodes to accept updates only from a sink node. Any update that is coming from untrusted sensor nodes will be considered as an invalid update. This way, sensor nodes can conserve more energy by dropping packets that are coming from unknown sensor or sink nodes attempting

to update the routing table.

V. Conclusion and Future Work

This paper presents the background of underwater protocols and their security threats. We focused on protecting protocols from MAC and routing attacks. By using the multi-factor authentication technique, underwater nodes will be able to detect malicious activities. Hence, utilizing network information as protection can defend against several attacks.

We are planning to model and develop the proposed approach and evaluate it in Network Simulator 2 (NS2). To test the efficiency of our proposed work, we will model Sybil, Wormhole, and flooding attacks. The evaluation will be based on the probability of detection, end-to-end delay, energy consumption, and PDR. Our goal is to ensure that packets can be successfully delivered with no modification through a transition and packets are 'available'whenever needed.

Acknowledgement

This work was partially supported by the Department of Computer Science and Graduate School of the University of Colorado Colorado Springs, King Faisal University, Saudi Arabian Cultural Mission (SACM) in the USA, and University of Tabuk.

References

[1] N. Nowsheen, G. Karmakar, and J. Kamruzzaman, "An Adaptive Approach to Opportunistic Data Forwarding in Underwater Acoustic Sensor Networks," *2014 IEEE 13th International Symposium on Network Computing and Applications*, pp. 229–236, 2014.

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

[3] A. Roy and N. Sarma, "Factors Affecting MAC Protocol Performance in Underwater Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 169, no. 5, pp. 36–41, 2017.

[4] S. Sahana, K. Singh, R. Kumar, and S. Das, "A Review of Underwater Wireless Sensor Network Routing Protocols and Challenges," *Next-Generation Networks*, pp. 505–512, 2018.

[5] D. N. Sandeep and V. Kumar, "Review on Clustering, Coverage and Connectivity in Underwater Wireless Sensor Networks: A Communication Techniques Perspective," *IEEE Access*, vol. 5, pp. 11 176–11 199, 2017.

[6] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, "Challenges and Security Issues in Underwater Wireless Sensor Networks," *Procedia Computer Science*, vol. 147, pp. 210–216, 2019. [Online]. Available: https://doi.org/10.1016/j.procs.2019.01.225

[7] S. S. Shahapur and R. Khanai, "Localization, routing and its security in UWSN - A survey," *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, pp. 1001–1006, 2016.

[8] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security Framework for Underwater acoustic sensor Networks," *OCEANS 2015 - Genova*, pp. 1–9, 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7271735/

[9] M. R. Ahmed, M. Aseeri, M. S. Kaiser, N. Z. Zenia, and Z. I. Chowdhury, "A novel algorithm for malicious attack detection in UWSN," *2nd International Conference on Electrical Engineering and Information and Communication Technology, iCEEiCT 2015*, no. May, pp. 21–23, 2015.

[10] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 729–752, 2019.

[11] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, and C. E. Chow, "A Survey on MAC Protocol Approaches for Underwater Wireless Sensor Networks," *IEEE Sensors Journal*, pp. 1–16, 2020.

[12] X. Li, G. Han, A. Qian, L. Shu, and J. Rodrigues, "Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks," *2013 21st International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2013*, 2013.

[13] T. Dargahi, H. H. Javadi, and H. Shafiei, "Securing Underwater Sensor Networks Against Routing Attacks," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2585–2602, 2017.

[14] G. Khan, K. K. Gola, and R. Rathore, "Robust data aggregation, encryption and data transfer in UWSNs," *Proceedings on 2015 1st International Conference on Next Generation Computing Technologies, NGCT 2015*, no. September, pp. 403–407, 2015.

[15] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," *2010 WRI International Conference on Communications and Mobile Computing, CMC 2010*, vol. 1, pp. 162–168, 2010.

[16] G. Toso, D. Munaretto, M. Conti, and M. Zorzi, "Attack Resilient Underwater Networks Through Software Defined Networking," *Proceedings of the International Conference on Underwater Networks & Systems*, pp. 44:1—-44:2, 2014. [Online]. Available: http://doi.acm.org/10.1145/2671490.2674589

[17] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[18] G. Yang, L. Dai, and Z. Wei, "Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks," *Sensors (Switzerland)*, vol. 18, no. 11, 2018.

[19] N. Goyal, L. Sapra, and J. K. Sandhu, *Energy-Efficient Underwater Wireless Communications and Networking*, 2020.

[20] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and Privacy in Localization for Underwater Sensor Networks," *IEEE Communications Magazine*, vol. 92, no. 1, pp. 1–1, 2015.