Array 13 (2022) 100117

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

Securing localization-free underwater routing protocols against depth-spoofing attacks

Ayman Alharbi [a,*], Alaa M. Abbas [b,c], Saleh Ibrahim [b,d]

[a] Department of Computer Engineering, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[b] Department of Electrical Engineering, Taif University, Haweyah, Saudi Arabia
[c] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[d] Department of Computer Engineering, Cairo University, Giza, Egypt

ARTICLE INFO

Keywords:
Underwater acoustic sensor networks
Routing protocols
Depth-based routing
Secure routing
Sinkhole attacks
Depth-spoofing attack

ABSTRACT

Localization-free depth-based opportunistic routing protocols are an energy efficient choice for underwater wireless sensor networks (UWSNs). However, most depth-based routing protocols are vulnerable to sinkhole attacks caused by depth spoofing. In this paper, we propose an energy-efficient depth-based probabilistic routing protocol (DPR) that is resilient against depth spoofing. By encouraging unqualified (suboptimal) relay nodes to randomly forward data packets, the adversarial effects of depth-spoofing can be mitigated. As the randomized forwarding probability increases, a better packet delivery ratio can be achieved when under depth-spoofing attacks. To keep energy consumption in check, we propose a simulation-based methodology for finding the optimal forwarding probability. By adjusting the unqualified node forwarding probability, the proposed DPR protocol can effectively resist depth-spoofing attacks with a reasonably efficient energy overhead. A delivery ratio exceeding 90% can be achieved under attack with energy overhead as low as 35% under normal conditions. In comparison with relevant existing protocols, the proposed protocol achieves better energy efficiency, resilience efficiency, and scalability.

1. Introduction

Securing underwater sensor networks (UWSNs) has gain considerable attention in recent years. This is due to the fact that security vulnerabilities are continuously exploited by adversaries and third parties for political and financial advantages [1]. A wide variety of attacks exist, with objectives ranging from sniffing the network [2] to disrupting or totally disabling operations [3]. UWSNs Routing protocols have been exposed to variety of several attacks [4]. Such attacks may affect the performance of the routing lightly or even completely. In this paper, we focus on securing the depth-based routing protocol (DBR) [5] against a selected proven attack. DBR protocol and its recent variants, such as [6–11] are particularly favorable for UWSNs due to that fact that they do not require full node localization, which is a challenging task in the underwater environment. The original DBR protocol, as well as its many derivatives, determines routes using one-dimensional depth information, which is easily obtainable by measuring pressure. In these protocols, the data generated by underwater nodes are collected by sinks placed at the water's surface. Each routing hop attempts to minimize the packet depth until it reaches a surface sink. Relay nodes hold packets received from the channel and wait for other nodes, which may be closer to the surface, giving them a chance to forward first. Nodes closer to the surface go first and announce their depth in the header of forwarded packets. Upon learning that a neighbor has already forwarded the held packet, it is assumed to be closer to the surface, and thereafter, deeper nodes discard their held copies.

One of the threats against DBR protocols techniques, the sinkhole attack. Unlike a denial-of-service attack that aims to overwhelm network resources, a sinkhole attack aims to inhibit the network from delivering valuable information [12]. It is considered one of the most critical and severe attacks, as it is very hard to observe [13] and can reduce the lifetime of the network by 70% [10].

Although the opportunistic behavior of DBR relay nodes saves energy, it enables a variant of the sinkhole attack called the depth-spoofing attack. An adversary can take advantage of the behavior pattern by convincing relay nodes in a certain neighborhood to drop their held packets prematurely. Since the work done by Ref. [14], it has been known that a carefully positioned adversary announcing a smaller depth

* Corresponding author.
E-mail address: aarharbi@uqu.edu.sa (A. Alharbi).

https://doi.org/10.1016/j.array.2021.100117
Received 10 August 2021; Received in revised form 8 October 2021; Accepted 2 December 2021
Available online 6 December 2021

can inhibit neighboring relay nodes from forwarding, thus causing a routing sinkhole.

Naïve secure routing approaches to resist this attack, such as cryptography-authenticated routing, e.g. Ref. [15], can be circumvented by a compromised node. Trust-based secure routing, as mentioned by Refs. [16,17], requires the exchange of second-hand information, which exhausts additional resources in the already constrained UAN resources. Some physical layer techniques, such as the estimation of the angle of arrival using vector acoustic sensors [18], can potentially help avoid depth-spoofing attacks. However, the additional cost and complexity of such elaborate physical layer technologies contradict the philosophy of the DBR protocol, which seeks to provide a low-cost localization-free routing protocol.

Motivated by the facts that (a) depth-based routing is one of the most successful classes of routing protocols in UANs, (b) depth-based routing is inherently susceptible to depth-spoofing vulnerability, and (c) the efficiency of existing countermeasures against depth-spoofing vulnerability is limited, we propose a new approach to mitigate depth-spoofing attacks. Our contribution to this work can be summarized in two points:

- We propose probabilistic forwarding as an effective countermeasure against depth-spoofing sinkhole attacks.
- We minimize the energy overhead of the proposed protocol by adjusting the forwarding probability according to the specific network deployment.

The protocol proposed in this paper attempts to achieve the following objectives: (a) to be simple to implement and analyze and to establish its effectiveness in thwarting the depth-spoofing attack; (b) to have minimal overhead when operating in normal conditions and also in the presence of a depth-spoofing attacker; (c) to be suitable for UANs with different node densities and traffic loads through proper setting of protocol parameters; and (d) to be applicable to a variety of opportunistic routing protocols, including DBR and its variants.

The rest of the paper is organized as follows: In Section 2, we review relevant background and related work on depth-based routing and then illustrate the attack model. In Section 3, we present the proposed protocol. In Section 4, we detail the evaluation methodology and the simulation settings to be used for evaluation. In Section 5, we present the simulation results, discuss our observations, and highlight the main findings. Finally, in Section 6, we present the concluding remarks and future work.

2. Background and related work

In this section, we review the traditional DBR protocol and its derivatives. We then present the specifications of depth-spoofing attacks and review previous attempts to secure DBR protocols against this type of attack.

2.1. Depth-based routing protocols

DBR [5] is a special class of geographic routing protocols. Instead of using nodes' full location information, DBR only needs one-dimensional depth information. Depth information is readily available through simple pressure sensors, unlike the daunting task of underwater localization required for other protocols, such as vector-based forwarding and its variants [19,20]. Another advantage of DBR is that no additional control traffic is needed. Coordination between nodes occurs when nodes announce their current depths to their neighbors within a special field in the header of forwarded packets.

2.1.1. Basic operation of DBR protocol

Upon learning of a neighbor's transmissions, a DBR node decides whether it is a qualified forwarder or not. A qualified forwarder is a node with a depth smaller than the sender's depth marked on the received packet header. Unqualified forwarders immediately drop the received packet. Qualified forwarders, on the other hand, keep them in a priority queue for a holding time, T_H, calculated by the following formula:

$$T_H = K(R - d), \tag{1}$$

where K is the constant of proportionality, defined as $K = 2\tau/\delta$, τ is the maximum propagation time, defined as $\tau = V/R$, V is the acoustic signal propagation speed, R is the node communication range, d is the advantage in depth due to this forwarder defined as $d = d_{sender} - d_{forwarder}$, and $\delta \in (0, R]$ is a constant that determines the maximum holding time. The smaller the value of δ is, the longer the maximum holding time will be.

This greedy strategy gives a qualified forwarder closer to the surface the chance to forward the received packet before the holding times of deeper qualified forwarders expire. If a packet is being held for later forwarding in a relay node and a duplicate of the same packet is received such that the node is no longer qualified to forward the recently received duplicate packet, the relay node drops the copy of the packet it held.

To identify copies of the same packet, DBR packet headers contain the source ID and a source-unique sequence number. Each relay node keeps track of all received packets using a local cache of (source ID, sequence number) pairs. Once a node decides to drop a packet, all copies of the same packet received later hit the local cache and are immediately dropped regardless of the sender's depth found in the header of the copy. Because of its low overhead cost, DBR is considered a practical answer to UAN challenges.

2.1.2. DBR adaptations

Due to the significant success of DBR, several adaptations of the protocol have been proposed in the literature. The energy-efficient depth-based routing (EEDBR) proposed in Ref. [21] aims to improve network lifetime by factoring nodes' residual energy into the forwarding decision. However, nodes are required to exchange depth and residual energy information regularly, which adds extra overhead. To address this, nodes keep depth and residual energy information regarding those neighbors with lesser depth and use that information to select a next-hop forwarder.

Similarly, the lightweight depth-based routing (LDBR) protocol proposed in Ref. [10] improves the overall lifetime of the network by following a similar strategy that lets nodes with residual energy lower than a preset threshold discard received packets, allowing other qualified forwarders with sufficient residual energy to step forward.

The interference-aware energy-efficient depth-based routing protocol proposed in Ref. [15] attempts to reduce potential interference between next-hop forwarders by factoring in node density in the neighborhood of each candidate relay node during the relay selection process.

The energy-efficient cooperative opportunistic routing (EECOR) protocol in Ref. [22] uses a fuzzy-logic approach to select a forwarding node from among neighbors. In addition to depth information, the relay selection process uses packet delivery probability and energy consumption ratio to determine the holding delay for each forwarder.

The RE-PBR routing protocol [23] enhances DBR and EEDBR routing strategies by incorporating other parameters, such as link quality, to determine the best candidate link based on the sender's neighboring node positions. In addition, to improve energy efficiency, RE-PBR selects only one neighbor to participate in the forwarding process and eliminates the holding time upon receiving packets.

The DBR forwarding decision was improved by considering the depth difference of two-hop neighbors in Refs. [6,24,25]. The WDFAD-DBR protocol proposed in Ref. [6] handles the uneven and sparse distribution of nodes by collecting two-hop depth information to guide relay selection. The protocol uses the history of neighbors in the neighbor's table to predict the neighbor's behavior and to improve network performance. Subsequently, RPSOR [25] enhanced the

WDFAD-DBR protocol by considering the depth differences, energy level, and the shortest path of forwarders. RPSOR calculates priority function, which is increased exponentially for small-depth differences of candidate forwarding nodes.

SORP [26] was developed based on a depth-routing mechanism to avoid void areas, which might exist in some topologies. The stateless routing protocol detects void regions, as well as local trapped nodes, and then avoids including them in the routing process.

Authors in Ref. [27] have proposed RSAR and CoSAR protocols based on depth information. RSAR reduces the burden of low-depth nodes by classifying nodes in the network into several energy grades. The deepest nodes will have higher energy grades, while nodes closest to the water surface will have smaller grades. Each source node calculates the weight based on depth, energy grade, and remaining energy of the next forwarding node. However, RSAR transmits packets using a single link, which may lead to unreliable delivery. To mitigate this issue, the CoSAR protocol depends on a cooperative forwarding mechanism.

To minimize end-to-end delay and achieve better network performance based on the depth routing technique, the authors of [28] proposed the DRADS, iDRADS, and Co-iDRADS delay sensitive routing protocols. Depth information is utilized in each protocol to assure a reliable link and short delivery time in the routing process.

A recently proposed Energy Efficient Depth-based Opportunistic Routing with Void Avoidance (EEDOR-VA) [29] uses a reactive routing mechanism to acquire a node hop count from a sink and combine this information with node depth to determine the node priority in the forwarding process. EEDOR-VA selects candidate forwarding sets to avoid routing voids and coordinates between nodes within the candidate set to reduce redundant transmissions.

Unfortunately, all the abovementioned DBR-variant protocols are susceptible to depth-spoofing attacks, which will be explained in the next subsection.

2.2. Depth-spoofing attack

This attack against depth-based routing is intended to cause a sinkhole-like effect, which prevents packet delivery. We adopt the attack model presented in Ref. [14], which makes the following assumptions:

a) Malicious and legitimate nodes have the same transmission range.

b) The adversary can place malicious nodes at the most damaging location in the network.

Fig. 1 illustrates how the depth-spoofing attack works. The source node *S* has one qualified forwarder *R*, which can transmit packets directly to sink *D*. The malicious node *A* is placed such that it can receive transmissions of *S* and all its neighbors, namely *R*. When *S* transmits a data packet, both *R* and *A* will pick it up, since they are all within the transmission range of *S*. The attacker will try to prevent *R* from forwarding the packet received from the source. While *R* will hold the packet for a short while in its transmission queue, *A* will quickly retransmit its copy of the packet announcing a fake depth that makes it look closer to the surface than *R* actually is. Consequently, *R* will drop its copy of the packet, which will effectively be lost.

The assumption that the malicious node has the same transmission range as the legitimate nodes can be justified: If the malicious node transmits the spoofed packets to a larger range than that reached by the source, the malicious node can inadvertently deliver the packet to the destination or at least to a relay node that is closer to the destination than the neighbors of the source. In this case, the malicious node will cooperate in the delivery process rather than disrupting it. Similarly, if the transmission range of the malicious node is smaller than that of the legitimate nodes, the depth-spoofed packet may not reach some of the neighbors of the source node, which allows them to successfully relay data packets to the destination. Therefore, the most effective depth-spoofing attack is possible when the transmission range of the attacker is close to the transmission range of the legitimate nodes.

2.3. Depth-spoofing attack mitigation mechanisms

A partial solution to the depth-spoofing attack was proposed by the resilient pressure-based routing (RPR) protocol in Ref. [8]. RPR, like DBR, uses depth information to determine packet holding times but employs cryptographic authentication and a sliding window threshold. During the forwarding decision, instead of comparing the depth advantage to a fixed minimum threshold, the received packet header will contain a lower bound threshold and an upper bound threshold. Only nodes within the threshold window are required to forward. Each sender determines the threshold window for the next hop by choosing two depths randomly from its neighbor list. The communication

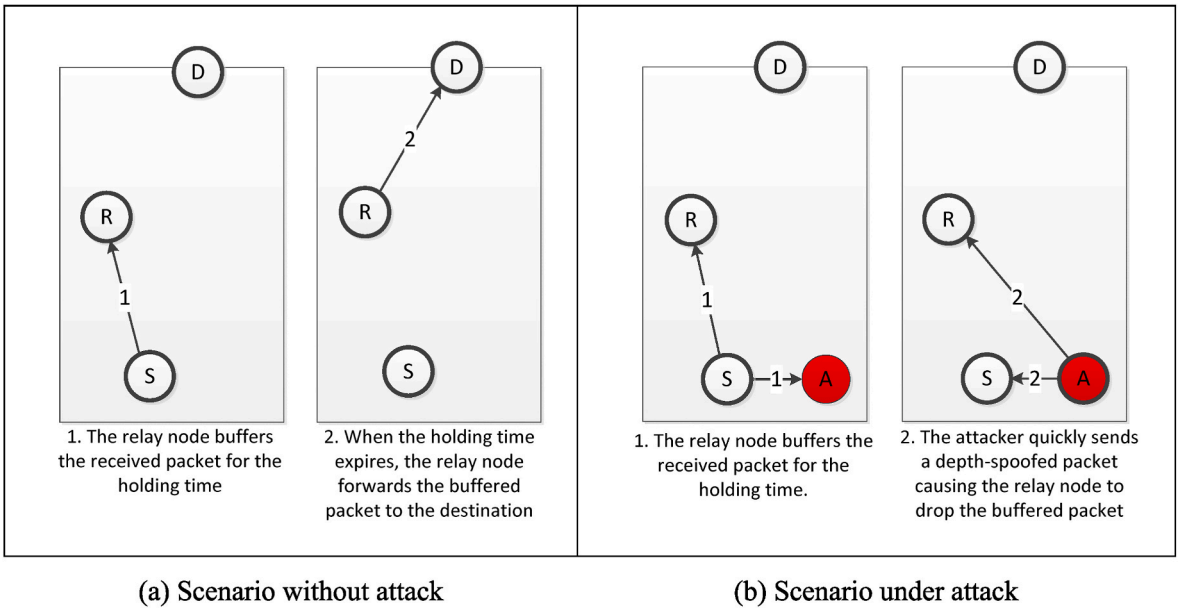


Fig. 1. Depth-spoofing attack. Attacker node ***A*** misleads relay node ***R*** into believing that the packet has already moved up towards the surface, thus inhibiting ***R*** from forwarding and causing a blackhole effect.

overhead of PRP is tremendous because randomized threshold windows tend to form routes with more hops than the purely opportunistic DBR. The increase in the number of packet transmissions per unique packet delivered can be up by 100%–300%, depending on the network density.

The recently proposed depth-based secure routing (DBSR) [15] uses cryptography to sign depth information within the routing headers. To reduce the overhead, DBSR employs a cryptographic signature to protect the integrity of only the routing headers. The use of a cryptographic authentication mechanism eliminates depth-spoofing by intruders, but the protocol remains wide open to depth-spoofing attacks by adversaries that can compromise nodes. Moreover, DBSR assumes that private signing keys are configured manually on each node, which increases the maintenance cost of a UAN in case new nodes need to be added to an existing deployment.

The SEECR [30] protocol was also developed to secure depth-based routing protocols. Each node compares its packet against a potential spoofed one using two queues. If the value of the attack threshold of any node is reached, then the protocol ignores this node in the routing process thereafter. However, since the attack model and relevant assumptions have not been clarified in this work, we have decided to compare the RPR protocol with our proposed DPR protocol.

3. Proposed protocol

To mitigate the effect of the depth-spoofing attack, we propose an improved version of the DBR protocol, called the depth-based probabilistic routing protocol (DPR). In this section, we specify the proposed routing protocol and analyze its expected behavior under depth-spoofing attacks as well as under normal conditions.

3.1. DPR specifications

The DPR packet header format is adopted from DBR without changes. Specifically, the first two fields of DPR represent the source address and source-unique sequence number, which are used to identify unique packets. The third field—the depth—indicates the last sending node depth.

Algorithm 1
Receive Packet from MAC

Inputs: received packet, P, current time, t, received packet cache, C, forwarding queue, Q, current node depth, D, and threshold for minimum depth advantage, d_{min}.
Outputs: Updated cache, C, and forwarding queue, Q.
Procedure:
$d \leftarrow P.depth - D$ ▷ *calculate depth gain*
if $C.contains(P.srcID,\ P.seqNo)$ ▷ *if the received packet already exists in the cache*
  if $Q.contains(P.srcID,\ P.seqNo)$ ▷ *if the received packet is already queued*
    $P' \leftarrow Q.get(P.srcID,\ P.seqNo)$ ▷ *obtain the old packet*
    if $d > d_{min}$ ▷ *if depth gain above the threshold*
      $t_H \leftarrow calculateHoldingTime(d)$ ▷ *using equation* (1)
      $t_F \leftarrow t + t_H$ ▷ calculate the forwarding time
      if $P'.timer.expires > t_F$ ▷ if the forwarding time is sooner than old forwarding time
        $P'.timer.expires \leftarrow t_F$ ▷ update queued packet forwarding time to the earlier time
      end if
    else if $d < 0$ ▷ if the duplicate packet was received from a sender closer to the surface
      $P'.dropFlag \leftarrow$ **true** ▷ mark the corresponding queued packet for dropping
    end if
  end if
else ▷ received fresh packet
  C.add$(P.srcID,\ P.seqNo)$ ▷ add received packet id to the cache
  if $d > d_{min}$ ▷ if depth gain above the threshold
    $t_H \leftarrow$calculateHoldingTime(d) ▷ using equation (1)
    $t_F \leftarrow t + t_H$ ▷ calculate the forwarding time
    $P.depth \leftarrow D$ ▷ update the packet depth
    $P.dropFlag \leftarrow$ **false** ▷ do not drop the packet yet
    $P.timer.expires \leftarrow t_F$ ▷ set the packet forwarding time
    $P.timer.start$ ▷ start the holding timer for forwarding the received packet
    $Q.add(P)$ ▷ insert the received packet at proper place in the holding queue
  end if
end if ∎

(*continued on next column*)

Algorithm 1 (*continued*)

Algorithm 2
Holding timer expires.

Inputs: held packet, P, forwarding queue, Q.
Outputs: forwarding decision $a \in \{forward,\ drop\}$.
if $P.dropFlag$ ▷ if packet is marked for dropping
  $x \leftarrow random([0,\ 1))$
  if $x < p$
    $a \leftarrow forward$ ▷ *forward with probability* p
  else
    $a \leftarrow drop$ ▷ *drop with probability* $1 - p$
  end if
  else ▷ *if not marked for dropping*
    $a \leftarrow forward$ ▷ *forward unconditionally*
end if
$Q.remove(P)$ ∎

The operation of DPR is controlled by a new parameter, p, which denotes the unqualified forwarding probability. The process of handling a packet received from the MAC layer and the process of finally forwarding a held packet at the scheduled time are listed as Algorithm 1 depicted in Fig. 2 and Algorithm 2 depicted in Fig. 3.

The main difference in DPR operation compared to traditional DBR is the action taken when a node receives a neighbor's retransmission of a packet that already exists in the node-forwarding queue. Traditionally, DBR drops a buffered packet when the newly received retransmission of the packet deems the node an unqualified forwarder, which allows an attacker to force forwarders to drop their packets. To solve this problem, the proposed DPR instead marks the buffered packet for future potential dropping. The final decision to drop the marked packet occurs after the holding timer of the marked packet expires. The proposed DPR makes a non-deterministic decision to forward the marked packet with probability p or to drop it with probability 1–p. The higher the value of p is, the more resilient the proposed protocol should be to depth-spoofing attacks. The adjustment of p will be studied in the following subsection.

3.2. Optimal unqualified forwarding probability

To determine the optimal value of the unqualified forwarding probability p or the forwarding probability for short, we first study the effect of p on the performance of the network in two cases: (a) under depth-spoofing attack and (b) under normal conditions.

When the network is under attack, each of the good forwarders within the attacker's communication range are called *vulnerable nodes*. When the attacker retransmits a packet with a spoofed depth, copies of the same packets found in the forwarding queues of vulnerable nodes are called *vulnerable packets*. DPR causes vulnerable nodes to keep vulnerable packets, which would have otherwise been dropped in DBR due to the depth-spoofing attack. Vulnerable nodes will only mark vulnerable packets for dropping but will eventually forward each of them with probability p. Therefore, the probability of dropping a vulnerable packet is $(1 - p)$. When the number of vulnerable nodes with a path to the sink is n, the depth-spoofing attack is successful if all vulnerable nodes simultaneously decide to drop the vulnerable packets. Therefore, the probability of a successful depth-spoofing attack is reduced to $(1 - p)^n$.

On the other hand, when the network is operating normally, probabilistic unconditional forwarding is expected to cause additional traffic. Namely, forwarders that become unqualified upon learning of their neighbors forwarding packets that already exist in their queues will still have a chance to forward each of these packets with probability p. The

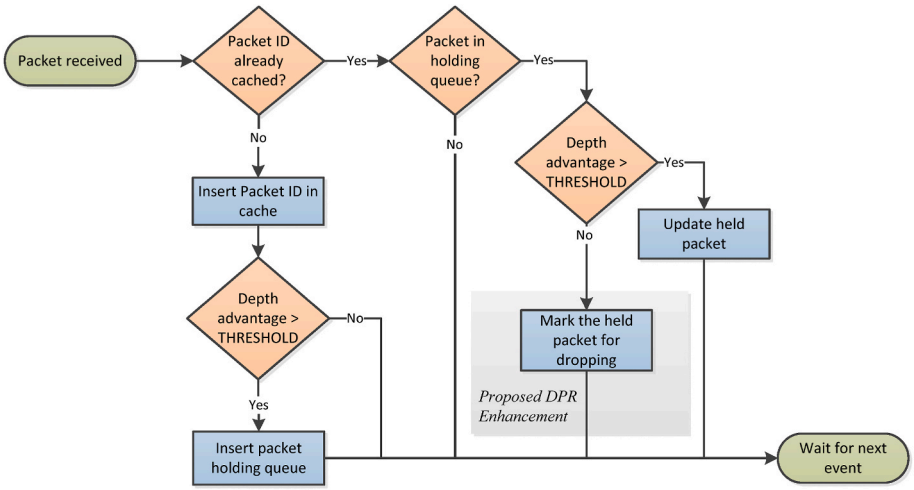


Fig. 2. Flowchart of Algorithm 1, performed when a packet is received from the MAC layer. The shaded area highlights the modification introduced in the proposed depth-based probabilistic routing protocol.

resulting potential multiple forwarding of the same packet increases the overhead and negatively affects the efficiency of the routing protocol. Therefore, it is important to analyze the overhead.

We estimate the communication overhead by finding the expected number of additional packets forwarded by DPR that would not be forwarded by DBR. If the qualified forwarder of a packet has m unqualified neighbors holding a copy of the same packet, then the expected number of additional forwarded packets is $(p \cdot m)$ packet. Unqualified forwarding neighbors is a subset of all neighbors within a node's communication range. Obviously, neighbors that have already forwarded a specific packet are no longer considered unqualified forwarders of that packet. Therefore, m can be much smaller than the node's degree (number of neighbors). Other factors can affect the number of successfully forwarded packets, such as the contention level and the MAC protocol in use. For example, if the transmissions of two or more unqualified forwarders happen to interfere, some or all of them may fail, thus causing no further traffic and reducing overhead. Therefore, the overhead caused by probabilistic forwarding is expected to be reasonably low.

To sum up the effect of the probability parameter p, there seems to be a trade-off between the achievable delivery ratio and the overhead due to the additional packets forwarded. It is expected that a large p improves delivery ratio when the network is under a depth-spoofing attack but also increases overhead when the network is not under attack. Due to the interplay between network topology, MAC protocol, and traffic load, we propose that the value of p be statically tailored for a given scenario using simulation. Given a specific UAN deployment, we simulate it with various values of p for each of the two cases: with attack and without attack. Two metrics are calculated—the delivery ratio r_p, and overhead, w_p—corresponding to each value of p. The delivery ratio r_p for a given forwarding probability p is calculated as follows:

$$r_p = \frac{D_p'}{D_0}, \tag{2}$$

where D_p' is the number of packets delivered by DPR under attack with the given forwarding probability, and D_0 is the number of packets delivered by DPR under normal conditions with $p = 0$, which is equivalent to the behavior of the original DBR. The overhead, w_p, is calculated as follows:

$$w_p = \frac{F_p}{F_0}, \tag{3}$$

where F_p is the total number of packets transmitted by all the nodes using DPR under normal conditions with the given forwarding probability, and F_0 is the total number of packets transmitted by all nodes using DPR under normal conditions with $p = 0$, which is equivalent to the behavior of the original DBR protocol.

To measure the efficiency of the proposed protocol in resisting the depth-spoofing attack, we define the resilience efficiency metric as follows:

$$\eta_p = \frac{r_p}{w_p} \times 100\%. \tag{4}$$

A higher resilience efficiency indicates the ability to achieve a higher delivery ratio when the network is under attack while keeping the overhead low when the network is operating normally. The forwarding probability p is chosen to maximize the network resilience efficiency.

4. Evaluation methodology and simulation

Since the main objective of an adversary launching a depth-spoofing black-hole attack is to cut off delivery, the delivery ratio should arguably be the key effectiveness indicator of the proposed countermeasure. The efficiency of the proposed approach can be demonstrated by showing that the additional forwarding overhead is limited. Excessive additional forwarding directly increases energy consumption and indirectly increases delay and reduces throughput. Therefore, showing that the additional forwarding overhead is marginal is sufficient to indicate that the negative effect of the proposed approach on the subsequent metrics (delay, throughput, and energy) is limited.

To evaluate the effectiveness and cost of the proposed probabilistic forwarding technique, we set up the following simulation scenario. We deployed the underwater nodes randomly in a volume of 500 m × 500 m × 250 m, where 250 m was the maximum depth. A single sink was placed at the center of the surface area. When placing underwater nodes, special care was taken to guarantee that the resulting network topology was always connected and that the node degree did not exceed the degree set for the corresponding network density.

For this simulation, the underwater node that was the farthest from the sink node was chosen as the source of traffic. The total number of underwater nodes varied according to the target network density and maximum node degree, and 100 different network topologies were generated corresponding to each network density in order to increase confidence in the results. Fig. 4 illustrates three sample networks corresponding to each of the three network densities and node degrees. The blue dots represent underwater relay nodes, the red dot represents the source, and the green dot represents the sink. The dotted lines represent

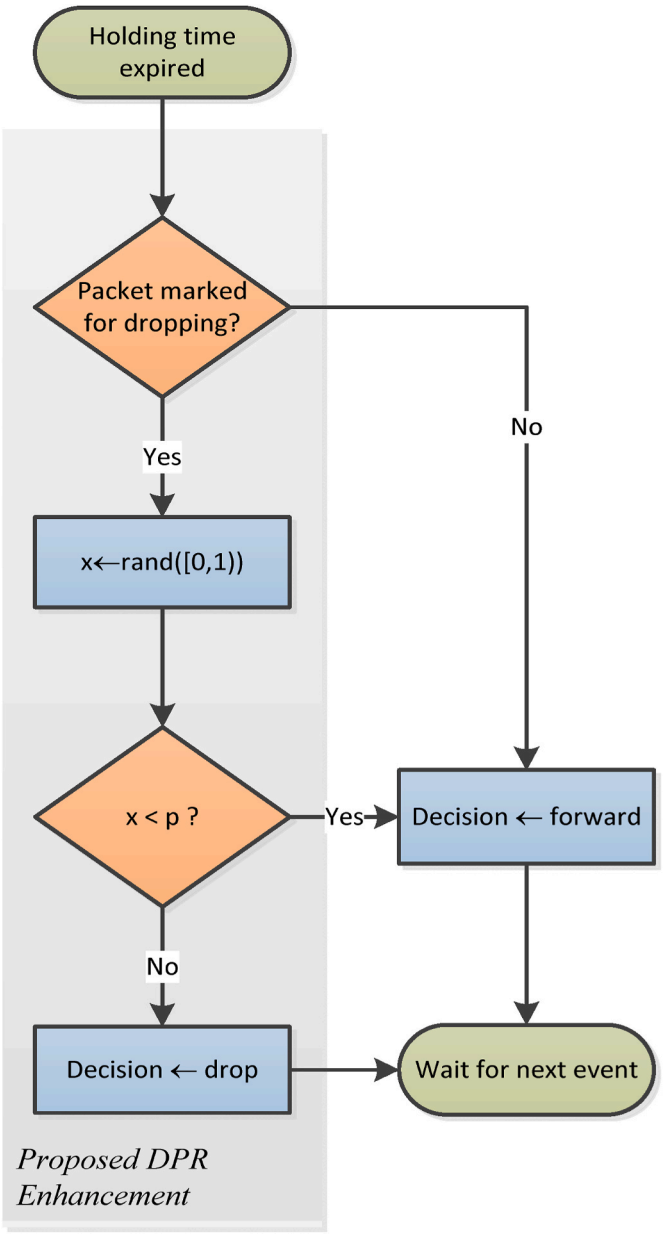


Fig. 3. Flowchart of Algorithm 2, performed when the timer for a packet held in the forwarding queue expires, in order to decide whether to forward or drop the packet. The shaded area highlights the modification introduced in the proposed depth-based probabilistic routing protocol.

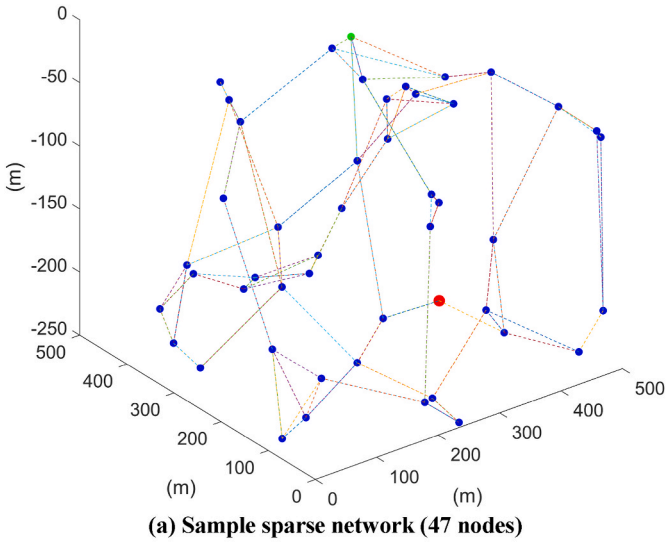
connectivity between nodes within each other's communication range.

One malicious node, performing a black-hole attack through depth-spoofing, was placed 1 m below the source node. This placement caused the attack to inhibit as many of the neighbors of the source node as possible from relaying source packets, thus enabling the attacker to launch a black-hole or gray-hole attack against the targeted source.

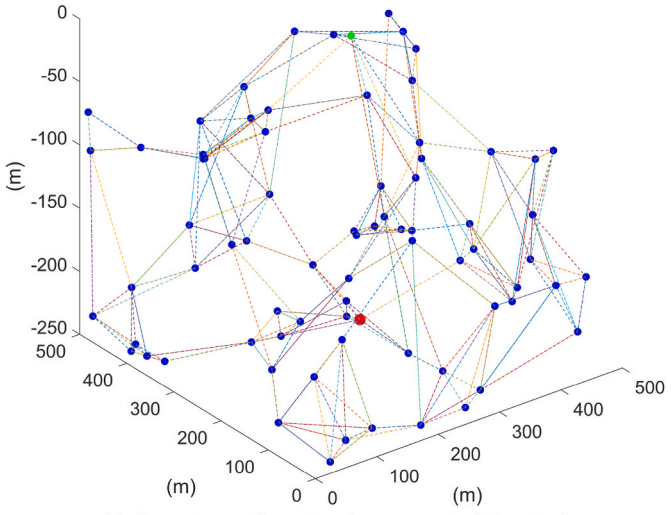
The simulation settings are summarized in Table 1. We adopted the physical layer model used in Ref. [29], which includes the path loss model, the absorption model, the ambient noise model, and the BPSK modulation bit-error-rate model, which are defined in Equations (5)–(8), respectively. Path loss is defined as follows:

$$A(f) = A_0 + 10\kappa \log_{10}(d) + d \times 10^{-3}\alpha(f) \quad (5)$$

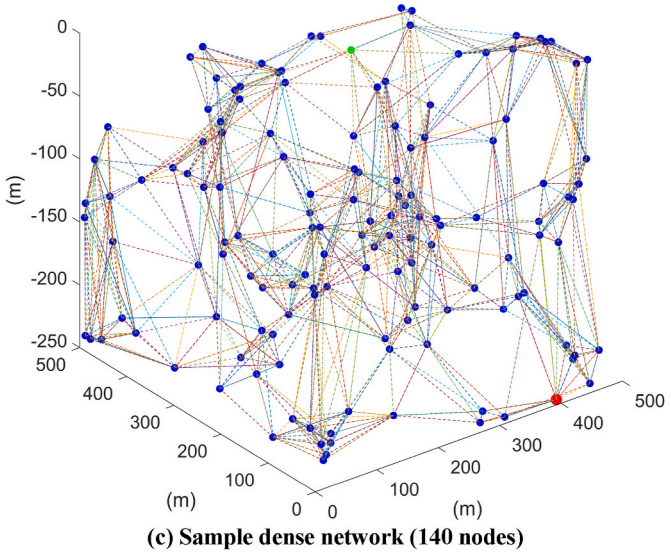
where f is the center frequency in kHz, $A_0 = 30\ dB$ is a normalizing constant, κ is the spreading factor, d is the distance in meters and a is the



(a) Sample sparse network (47 nodes)



(b) Sample medium density network (75 nodes)



(c) Sample dense network (140 nodes)

Fig. 4. Sample networks with different node densities.

Table 1
Simulation settings.

Parameter	Setting		
Deployment space	500 m × 500 m × 250 m deep		
Network density	sparse	medium	dense
— Number of nodes	47	75	150
— Max. node degree	5	8	15
— Number of simulated topologies	100	100	100
Channel model	Spherical spreading, additive noise		
Communication range	150 m		
Bit rate	12.5 Kbit/s		
Data generation rate	10 Byte/s		
Packet payload	50 Bytes		
Total data transmitted	100 packets		
MAC	ALOHA		

absorption coefficient, which is further defined as follows:

$$\alpha(f) = \frac{0.11f^2}{1+f^2} + \frac{44f^2}{4100+f^2} + 2.75\times 10^{-4} f^2 + 0.003 \text{ dB} \Big/ \text{km} \quad (6)$$

We simulated the spherical spreading by setting the spreading factor $\kappa = 2$ in Equation (5). The ambient noise can be approximated by the following power spectral density:

$$N(f) = 50 - 18\log_{10}(f) \quad (7)$$

The signal-to-noise ratio can be calculated using the following formula:

$$\gamma(f) = SL - N(f) - A(f)$$

where SL is the acoustic transmission power in dB. The electrical power transmission P_t in Watts is defined as

$$P_t = 2\pi z_d \times 0.67 \times 10^{-18} \times 10^{0.1\,SL}$$

where z_d is the ocean depth in meters. Assuming BPSK modulation, the average bit error probability is calculated as follows:

$$\varepsilon = \frac{1}{2}\left(1 - \sqrt{\frac{10^{0.1\,\gamma(f)}}{1+10^{0.1\,\gamma(f)}}}\right) \quad (8)$$

Therefore, the probability of successful reception of a packet of length m bits is $(1-\varepsilon)^m$. Transducers were configured with a bit rate of 12.5 Kbps. The transmission power was adjusted such that the nominal communication range is 150 m.

In our simulations, we adopted a basic ALOHA MAC protocol, in which packets are transmitted immediately regardless of the state of the channel and frames lost due to collisions are not retransmitted. ALOHA is a practical alternative in acoustic underwater MAC, considering the extremely high propagation delay, which renders synchronized protocols impractical [34]; hence, ALOHA has been frequently employed in UAN literature, such as [31].

Traffic was generated at a rate of 10 bytes per second, whereas each packet held a 50-byte payload. Thus, one packet was generated every 5 s. The source was configured to stop after transmitting exactly 100 packets, and the simulation was run for as long as it took for all the traffic caused by these messages to disappear from the network.

The number of packets delivered to the sink, $D_p^{'}$, was observed and divided by the corresponding ideal number of traditional DBR in the absence of the malicious attacker to obtain the delivery ratio, r_p, as defined in (2).

For each of the three network densities, four sets of scenarios were simulated: (a) DBR protocol with the attacker inactive, (b) DBR protocol with the attacker active, (c) DPR protocol with the attacker inactive, and (d) DPR protocol with the attacker active. When DPR was used, the simulation was repeated with various values of forwarding probability, ranging from $p = 0.1$ to $p = 1$. In each scenario, the experiment was repeated for each of the 100 generated network topologies and the mean result was reported.

The simulation model was developed in Java with a MATLAB scripting interface. The software package, available online at [32], can easily be used to reproduce the results presented in the following section.

5. Results and discussion

In this section, we elucidate the effect of the forwarding probability parameter p on the performance of the proposed DPR under different network conditions. Then, we compare the proposed protocol with existing relevant protocols.

5.1. DPR resistance to depth-spoofing attacks

To demonstrate the resistance of the proposed DPR protocol against depth-spoofing attacks, we simulated the sample networks in the presence of an active attacker and observed the packet delivery ratio r_p at each value of p. The results are shown in Fig. 5. The delivery ratios are calculated as a percentage of the ideal case of DBR under no attack using (2). In all three networks, depth-spoofing successfully created a sinkhole that hindered the delivery of packets. As the unqualified forwarding probability p increased, DPR successfully delivered more packets. The packet delivery ratio exceeded 90% when $p \geq 0.9$, $p \geq 0.7$ and $p \geq 0.4$, for the sparse, medium density, and dense networks, respectively. In effect, probabilistic forwarding has the potential to reduce or even eliminate the sinkhole effect of depth-spoofing attacks. As observed in Fig. 5, the denser a network is, the lower will be the forwarding probability needed to achieve a certain delivery ratio.

5.2. DPR overhead

Increasing the forwarding probability p increased the overall number of packets transmitted by DPR. Fig. 6 shows the overhead of DPR w_p as defined by (3), at various forwarding probabilities p. In all three networks, the overhead of DPR increased monotonically with p. The worst-case overhead in sparse, medium, and dense networks were less than 39%, 66%, and 61%, respectively. Therefore, the overhead increased with network density, confirming our earlier analysis that a larger number of suboptimal unqualified nodes are involved in probabilistic forwarding. The results indicate that networks with lower node density can tolerate higher forwarding probabilities with lower overhead compared to higher density networks.

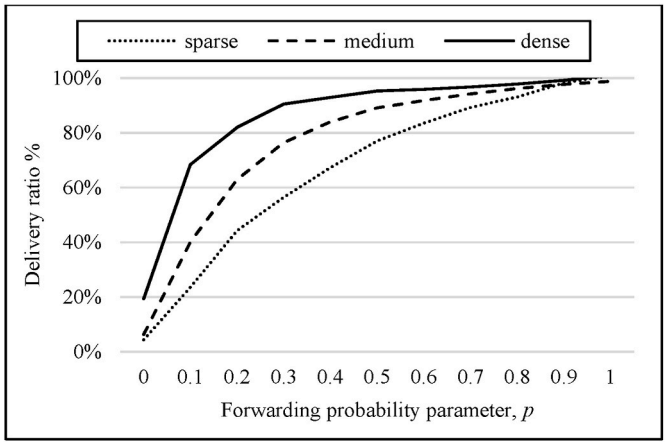


Fig. 5. Without probabilistic forwarding, no packets can be delivered under the depth-spoofing attack. Using a higher forwarding probability p improves the packet delivery ratio for networks of all densities. The higher the network density, the faster the improvement in packet delivery ratio.

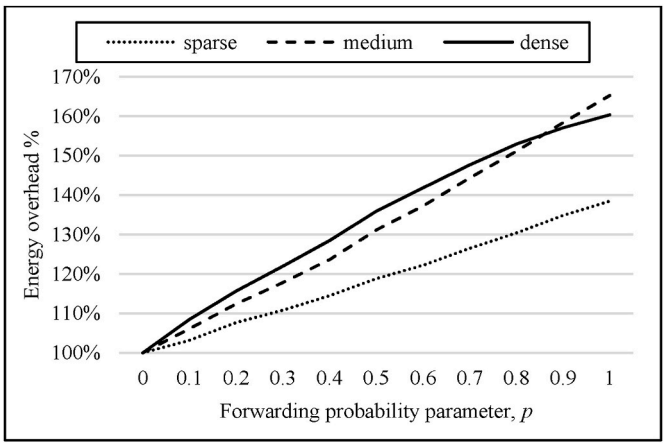


Fig. 6. Effect of forwarding probability on delivery cost in the absence of depth-spoofing attack, with varying node densities.

5.3. Adjusting the forwarding probability

The performance of DPR exhibited a tradeoff between resistance to depth-spoofing attacks represented by the packet delivery ratio and the overhead represented by the delivery cost. The optimal forwarding probability should maximize the resilience efficiency defined in (4).

Fig. 7 illustrates how the optimal resilience efficiency is affected by the network density. In the sparse network, where the overhead is significantly limited, it seems that the delivery ratio is the overwhelming factor affecting resilience efficiency. Therefore, the best resilience efficiency was achieved at a very high forwarding probability, $p = 0.9$. In denser networks, however, the overhead played a more significant role and pushed the optimal forwarding probability lower. In the medium density network, the optimal forwarding probability was $p = 0.5$, whereas in the dense network, it was $p = 0.3$. From this observation, we can confirm that networks with higher node densities are expected to achieve better security/efficiency balance with DPR at lower values of forwarding probability p.

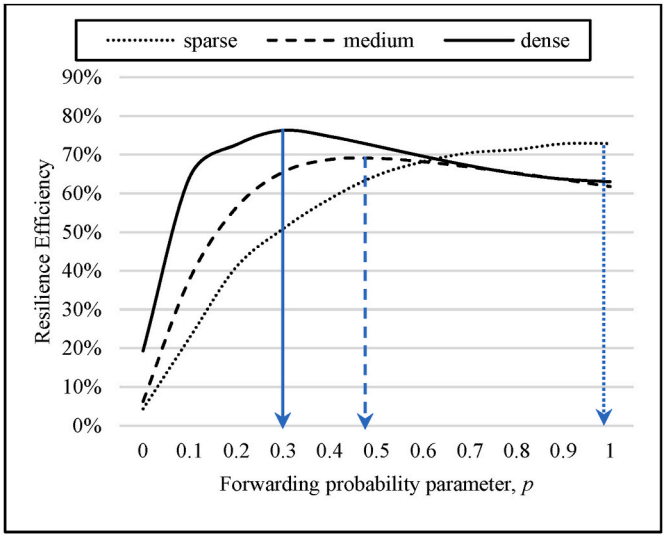


Fig. 7. Finding the optimal forwarding probability using the resilience efficiency, η. In the sparse network (a), the maximum η is at $p = 0.9$. In the medium-density network (b), the maximum η is at $p = 0.5$. In the dense network (c), the maximum η is at $p = 0.3$.

5.4. Comparison with existing protocols

In this section, we compare the proposed DPR protocol with existing relevant protocols. As mentioned earlier, DBSR [15] provides a partial solution to the depth-spoofing attack using cryptography but remains vulnerable in case of node compromise. Another limitation of DBSR comes from the key assignment problem, which causes a scalability issue. To demonstrate the effectiveness and efficiency of the proposed DPR protocol, we compare its performance with the existing RPR protocol [8] in terms of packet resilience efficiency, energy overhead, network lifetime, and end-to-end delay.

5.4.1. Energy efficiency comparison

Based on the assumption that all packets are transmitted at the same transmission power level, the energy efficiency of the network can be indicated by the number of delivered packets as a ratio of the total number of packet transmissions under normal conditions. Table 2 lists the average number of packet transmissions per delivered packet for each of the DBR, RPR, and the proposed DPR protocols for every simulated network. For instance, when the high-density network is operating normally, DBR costs the network about 47 packet transmissions per delivered packet, and RPR costs the networks 113 packet transmissions per delivered packet, whereas the proposed DPR costs the network only 50 packet transmissions per delivered packet. To compare the efficiency of the depth-spoofing countermeasures introduced by RPR and DPR, the energy efficiency of the original DBR is taken as a reference, and the energy efficiencies of DPR and RPR are calculated as a percentage of the DBR energy efficiency. The energy efficiency of the proposed DPR is compared to RPR in Fig. 8. Clearly, the proposed DPR has superior energy efficiency compared to RPR. The results also showed that the proposed DPR protocol has a slightly lower energy efficiency than the original insecure DBR protocol. This little energy overhead is justifiable by the significant security advantage of DPR against depth-spoofing attacks, as will be shown in the next subsection.

5.4.2. Resilience efficiency comparison

Resilience efficiency, defined in (4), indicates the energy efficiency of the depth-spoofing avoidance mechanism. The simulation results, shown in Fig. 9, indicate that when the proposed DPR protocol is operating at the optimal forwarding probability, the DPR resilience efficiency surpasses that of RPR. In both cases, the network under a depth-spoofing attack delivers a significant fraction of packets. However, due to the lower energy efficiency of RPR, a great amount of energy is spent delivering each packet even when the network is under normal conditions. This indicates that the proposed DPR strikes a better balance between achieving a high delivery ratio when the network is under attack and the energy cost when the network is not under attack.

5.4.3. Network lifetime comparison

We adopted the network lifetime definition given by Ref. [21], which focuses on the first depleted node as an indicator of the network lifetime. We assume that the network is homogenous (all nodes have the same battery capacity and the same transmission power), and all packets have fixed sizes. Therefore, the node depletion rate is proportional to the packet transmission rate, and the first depleted node is the node that makes the most frequent transmissions. To facilitate the comparison, we define the node depletion rate as follows:

Table 2
Number of packets transmitted per delivered packet under normal conditions.

	DBR	RPR	Proposed DPR
Sparse network	17.95	41.74	24.64
Medium density Network	28.02	63.51	32.73
Dense network	46.92	113.34	50.23

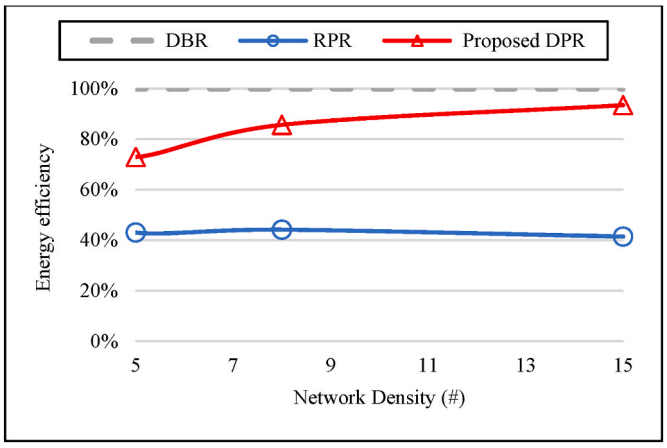


Fig. 8. Energy efficiency of depth-spoofing countermeasures in the absence of an attacker. Energy efficiency is represented as a percentage of the energy efficiency of the original DBR.

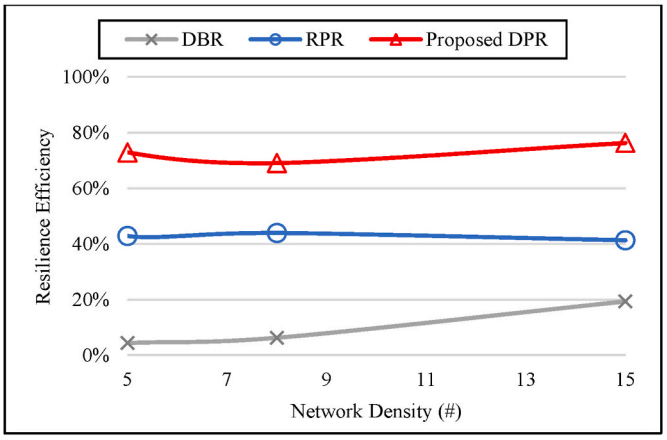


Fig. 9. Comparison of resilience efficiency.

$$\textit{Node depletion rate} = \frac{\textit{Numberof node transmissions}}{\textit{Number of delivered packets}}$$

We take the node depletion rate of DBR as a reference and hence represent the network lifetime as a fraction of the corresponding DBR network lifetime. As shown in Fig. 10, the proposed DPR keeps the lifetime of the network above 95% of the DBR lifetime, whereas RPR reduces the network lifetime to approximately 40%.

5.4.4. End-to-end delay comparison

End-to-end delay is the time spent delivering an application message from a source to a destination/sink node. As shown in Fig. 11, the effect of the proposed DPR on end-to-end delay is insignificant regardless of the network density.

6. Conclusion

In this paper, we proposed a security improvement to secure DBR against depth-spoofing sinkhole attacks using non-deterministic forwarding. The simulation showed that the proposed DPR protocol is potent against depth-spoofing sinkhole attacks. Since energy consumption is of utmost importance in underwater networks, the proposed protocol was also shown to have a limited energy overhead. Compared to its main competitor, RPR, the proposed DPR has approximately double the energy efficiency. The DPR also has a negligible effect on end-to-end delay. Since the performance of DPR is determined by the

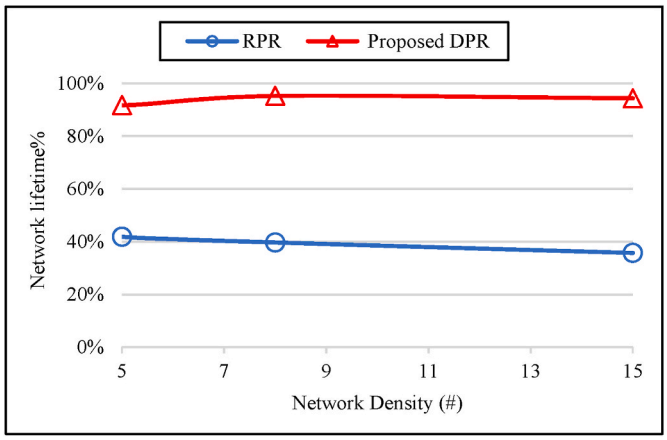


Fig. 10. Network lifetime comparison.

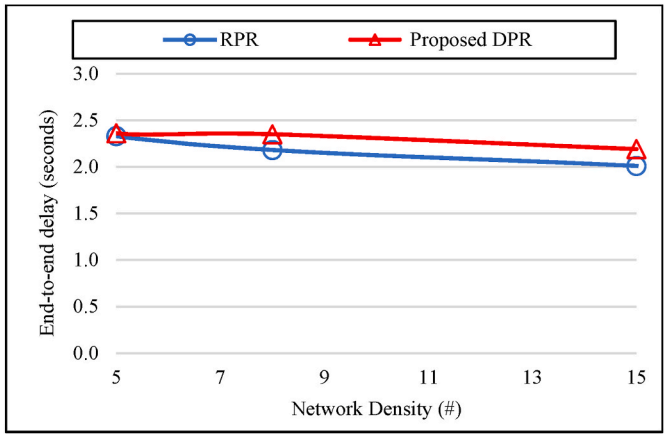


Fig. 11. End-to-end delay comparison.

forwarding probability parameter, we proposed a methodology for adjusting the forwarding probability for a specific network topology using simulation. However, using a constant forwarding probability for all nodes and for the entire duration of deployment may sometimes be suboptimal. Therefore, there is room for further improvement of network performance by dynamically adjusting the forwarding probability. Moreover, the proposed DPR can further be improved by considering the residual energy of each node to determine the forwarding probability in order to attempt to extend the network lifetime. Recently [33], presented a Master-Slave Architecture for UAN routing to reduce channel contention by designating master nodes as the only potential forwarders. Incorporating such an architecture within the proposed DPR protocol can also be considered. These improvements are left for future research.

Credit author statement

Ayman Alharbi: Conceptualization, Investigation, Writing – Original Draft, Visualization, Funding Acquisition. Alaa M. Abbas: Validation, Writing – Review & Editing. Saleh Ibrahim: Conceptualization, Methodology, Software, Investigation, Writing – Original Draft, Visualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported by the Deanship of Scientific Research at Umm Al-Qura University, grant code 19-COM-1-01-0019.

References

[1] Yang G, Dai L, Si G, Wang S, Wang S. Challenges and security issues in underwater wireless sensor networks. Procedia Computer Science 2019;147:210–6. https://doi.org/10.1016/j.procs.2019.01.225.
[2] T. Dargahi, H. H. S. Javadi, and H. Shafiei, "Securing underwater sensor networks against routing attacks," Wireless Pers Commun, vol. 96, no. 2, pp. 2585-2602, 2017/09/01 2017, doi: 10.1007/s11277-017-4313-1.
[3] Signori A, et al. Jamming the underwater: a game-theoretic analysis of energy-depleting jamming attacks. Atlanta, GA, USA. In: Presented at the proceedings of the international conference on underwater networks & systems; 2019. https://doi.org/10.1145/3366486.3366546 [Online]. Available:.
[4] Jiang S. On securing underwater acoustic networks: a survey. IEEE Communications Surveys & Tutorials 2019;21(1):729–52. https://doi.org/10.1109/COMST.2018.2864127.
[5] Yan H, Shi Z, Cui J-H. DBR: depth-based routing for underwater sensor networks. In: NETWORKING 2008 ad hoc and sensor networks, wireless networks, next generation internet, vol. 4982. Berlin, Heidelberg: Springer Berlin Heidelberg; 2008. p. 72–86 (Lecture Notes in Computer Science.
[6] Yu H, Yao N, Wang T, Li G, Gao Z, Tan G. WDFAD-DBR: weighting depth and forwarding area division DBR routing protocol for UASNs. Ad Hoc Netw 2016;37:256–82. https://doi.org/10.1016/j.adhoc.2015.08.023.
[7] Javaid N, Jafri MR, Khan ZA, Qasim U, Alghamdi TA, Ali M. iAMCTD: improved adaptive mobility of courier nodes in threshold-optimized DBR protocol for underwater wireless sensor networks. Int J Distributed Sens Netw 2014;10(11):213012. https://doi.org/10.1155/2014/213012.
[8] M. Zuba, M. Fagan, S. Zhijie, and C. Jun-Hong, "A resilient pressure routing scheme for underwater acoustic networks," Dec 2014 2014, no. Conference Proceedings: IEEE, pp. 637-642, doi: 10.1109/GLOCOM.2014.7036879. [Online]. Available: https://ieeexplore.ieee.org/document/7036879.
[9] Shah M, Javaid N, Imran M, Guizani M, Khan ZA, Qasim U. Interference aware inverse EEDBR protocol for underwater WSNs. Conference Proceedings: IEEE; Aug 2015 2015. p. 739–44. https://doi.org/10.1109/IWCMC.2015.7289175 [Online]. Available: https://ieeexplore.ieee.org/document/7289175.
[10] Gul S, Jokhio SH, Jokhio IA. Light-weight depth-based routing for underwater wireless sensor network. Conference Proceedings: IEEE; Feb 2018 2018. p. 1–7. https://doi.org/10.1109/ICACS.2018.8333483 [Online]. Available: https://ieeexplore.ieee.org/document/8333483.
[11] Ahmed T, Chaudhary M, Kaleem M, Nazir S. Optimized depth-based routing protocol for underwater wireless sensor networks. Conference Proceedings: IEEE; Dec 2016 2016. p. 147–50. https://doi.org/10.1109/ICOSST.2016.7838592 [Online]. Available: https://ieeexplore.ieee.org/document/7838592.
[12] Nithiyanandam N, Parthiban L. An efficient voting based method to detect sink hole in wireless acoustic sensor networks. Int J Speech Technol 2020;23(2):343–54. https://doi.org/10.1007/s10772-020-09700-3. 2020/06/01.
[13] Kala PC, Agrawal AP, Sharma RR. A novel approach for isolation of sinkhole attack in wireless sensor networks. 29-31 Jan. 2020. In: 2020 10th international conference on cloud computing. Confluence: Data Science & Engineering; 2020. p. 163–6. https://doi.org/10.1109/Confluence47617.2020.9057981.
[14] Zuba M, Fagan M, Jun-Hong C, Zhijie S. A vulnerability study of geographic routing in Underwater Acoustic Networks. Oct 2013. Conference Proceedings: IEEE; 2013. p. 109–17. https://doi.org/10.1109/CNS.2013.6682698 [Online]. Available: https://ieeexplore.ieee.org/document/6682698.
[15] Alharbi A. DBSR: a depth-based secure routing protocol for underwater sensor networks. Int J Adv Comput Sci Appl 2020;11(9). https://doi.org/10.14569/ijacsa.2020.0110974.
[16] Jinfang J, Guangjie H, Lei S, Chan S, Kun W. A trust model based on cloud theory in underwater acoustic sensor networks. IEEE Transactions on Industrial Informatics 2017;13(1):342–50. https://doi.org/10.1109/TII.2015.2510226.
[17] Han G, Jiang J, Shu L, Guizani M. An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network. IEEE Trans Mobile Comput 2015;14(12):2447–59. https://doi.org/10.1109/TMC.2015.2402120.
[18] Bereketli A, Guldogan MB, Kolcak T, Gudu T, Avsar AL. Experimental results for direction of arrival estimation with a single acoustic vector sensor in shallow water. Journal of Sensors 2015:401353. https://doi.org/10.1155/2015/401353. 2015/05/19 2015.
[19] Xie P, Cui J-H, Lao L. VBF: vector-based forwarding protocol for underwater sensor networks. In: Networking 2006. Networking technologies, services, and protocols; performance of computer and communication networks; mobile and wireless communications systems, vol. 3976. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. p. 1216–21 (Lecture Notes in Computer Science.
[20] Barenco Abbas CJ, Montandon R, Sandoval Orozco AL, Garcia Villalba LJ. EBVBF: energy balanced vector based forwarding protocol. IEEE Access 2019;7:54273–84. https://doi.org/10.1109/ACCESS.2019.2913026.
[21] Wahid A, Kim D. An energy efficient localization-free routing protocol for underwater wireless sensor networks. Int J Distributed Sens Netw 2012;8(4):307246. https://doi.org/10.1155/2012/307246.
[22] Rahman MA, Youngdoo L, Insoo K. EECOR: an energy-efficient cooperative opportunistic routing protocol for underwater acoustic sensor networks. IEEE Access 2017;5:14119–32. https://doi.org/10.1109/ACCESS.2017.2730233.
[23] Khasawneh A, Latiff MSBA, Kaiwartya O, Chizari H. A reliable energy-efficient pressure-based routing protocol for underwater wireless sensor network. Wireless Network 2018;24(6):2061–75. https://doi.org/10.1007/s11276-017-1461-x. 2018/08/01.
[24] Zhang M, Cai W. Energy-efficient depth based probabilistic routing within 2-hop neighborhood for underwater sensor networks. IEEE Sensors Letters 2020;4(6):1–4. https://doi.org/10.1109/LSENS.2020.2995236.
[25] Ismail M, et al. Reliable path selection and opportunistic routing protocol for underwater wireless sensor networks. IEEE Access 2020;8:100346–64. https://doi.org/10.1109/ACCESS.2020.2992759.
[26] Ghoreyshi SM, Shahrabi A, Boutaleb T. A stateless opportunistic routing protocol for underwater sensor networks. Wireless Commun Mobile Comput 2018:8237351. https://doi.org/10.1155/2018/8237351. 2018/11/11 2018.
[27] Ali M, Khan A, Mahmood H, Bhatti N. Cooperative, reliable, and stability-aware routing for underwater wireless sensor networks. Int J Distributed Sens Netw 2019;15(6). https://doi.org/10.1177/1550147719854249. 1550147719854249, 2019/06/01.
[28] Javaid N, Shakeel U, Ahmad A, Alrajeh N, Khan ZA, Guizani N. DRADS: depth and reliability aware delay sensitive cooperative routing for underwater wireless sensor networks. Wireless Network 2019;25(2):777–89. https://doi.org/10.1007/s11276-017-1591-1. 2019/02/01.
[29] Mhemed R, Comeau F, Phillips W, Aslam N. Void avoidance opportunistic routing protocol for underwater wireless sensor networks. Sensors 2021;21(6). https://doi.org/10.3390/s21061942.
[30] Saeed K, Khalil W, Ahmed S, Ahmad I, Khattak MNK. SEECR: secure energy efficient and cooperative routing protocol for underwater wireless sensor networks. IEEE Access 2020;8:107419–33. https://doi.org/10.1109/ACCESS.2020.3000863.
[31] Torres D, Friedman J, Schmid T, Srivastava MB, Noh Y, Gerla M. Software-defined underwater acoustic networking platform and its applications. Ad Hoc Netw 2015;34:252–64. https://doi.org/10.1016/j.adhoc.2015.01.010. 2015/11/01/.
[32] Ibrahim S. Underwater acoustic network simulator (UANSim). Oct, https://github.com/Saleh860/UANSim; 2021.
[33] Jan S, et al. Investigating master–slave architecture for underwater wireless sensor network. Sensors 2021;21(9). https://doi.org/10.3390/s21093000.