[Array 13 (2022) 100117](https://doi.org/10.1016/j.array.2021.100117)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Contents lists available at ScienceDirect |  |
| Array |
| journal homepage: [www.sciencedirect.com/journal/array](https://www.sciencedirect.com/journal/array) |

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

Ayman Alharbia,\*, Alaa M. Abbasb,c, Saleh Ibrahimb,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*

|  |  |
| --- | --- |
| A R T I C L E I N F O | A B S T R A C T |
| *Keywords:*  Underwater acoustic sensor networks Routing protocols  Depth-based routing  Secure routing  Sinkhole attacks  Depth-spoofing attack | 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, resil-ience efficiency, and scalability. |

**1. Introduction**

Securing underwater sensor networks (UWSNs) has gain consider-able attention in recent years. This is due to the fact that security vul-nerabilities 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 informa-tion, which is easily obtainable by measuring pressure. In these pro-tocols, the data generated by underwater nodes are collected by sinks placed at the water’s surface. Each routing hop attempts to minimize the

\* Corresponding author.

*E-mail address:* [aarharbi@uqu.edu.sa](mailto:aarharbi@uqu.edu.sa) (A. Alharbi).

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 en-ergy, 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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| <https://doi.org/10.1016/j.array.2021.100117>  [Received 10 August 2021; Received in revise](https://doi.org/10.1016/j.array.2021.100117)d form 8 October 2021; Accepted 2 December 2021  Available online 6 December 2021  2590-0056/© 2021 The Authors. Published by Elsevier Inc. This is an open | access | article | under | the | CC | BY-NC-ND | license |

(<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

*A. Alharbi et al.*  *Array 13 (2022) 100117*

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 vulnera-bility 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 opportu-nistic 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 pro-tocol. 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 de-rivatives. 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 locali-zation 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

2

*A. Alharbi et al.*  *Array 13 (2022) 100117*

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 for-warding 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 perfor-mance based on the depth routing technique, the authors of [28] pro-posed 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 for-warding 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.

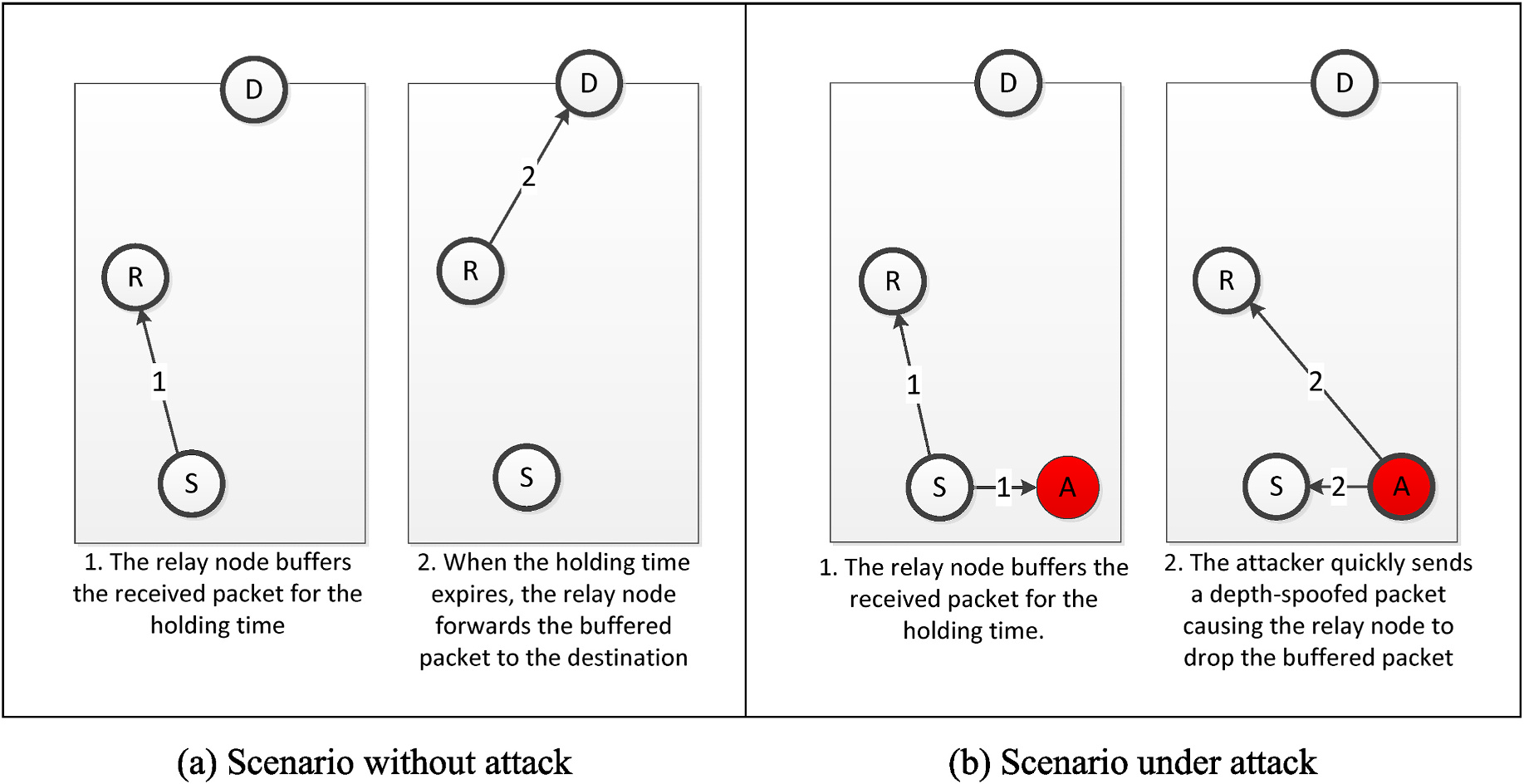
b) The adversary can place malicious nodes at the most damaging location in the network.

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 for-warding 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.

3

*A. Alharbi et al.*  *Array 13 (2022) 100117*

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 as-sumptions 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 probabi-listic 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.

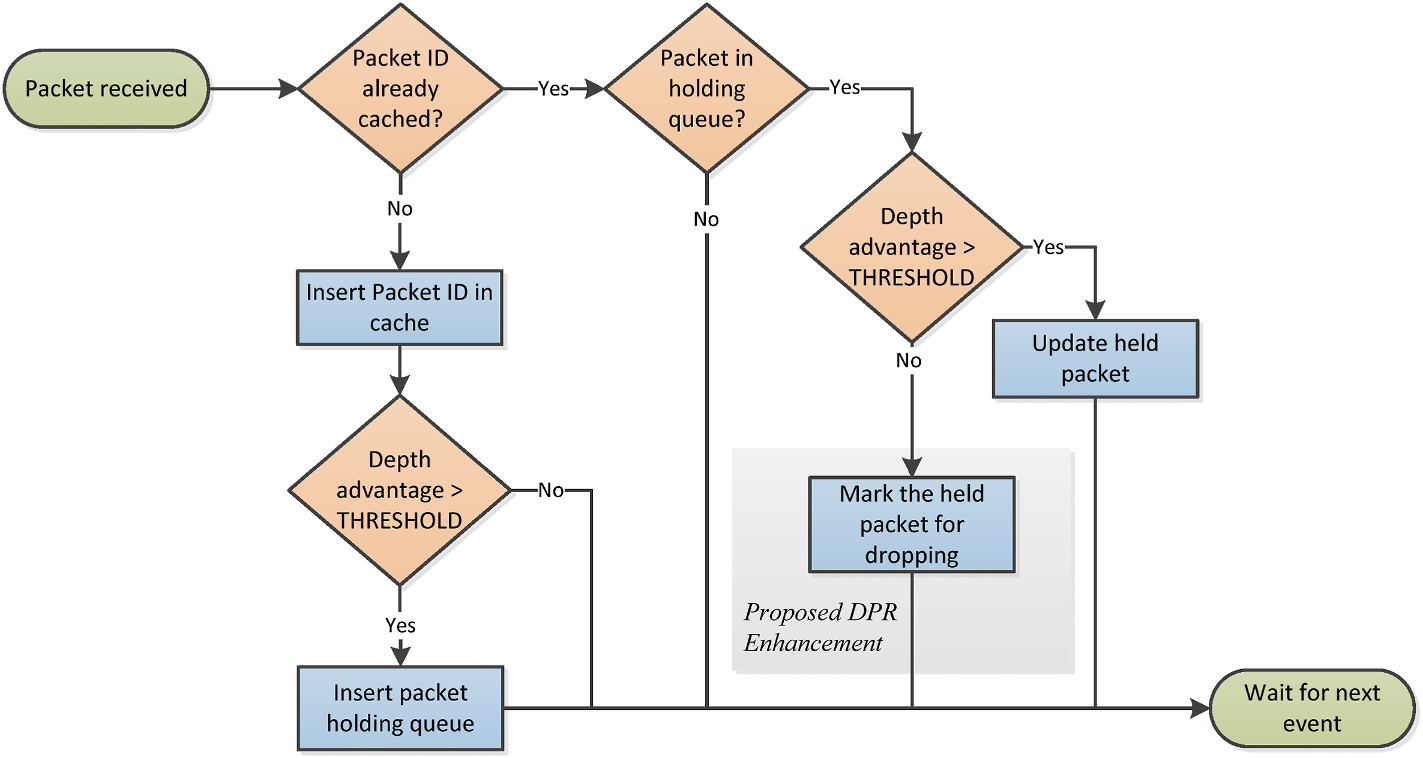
**Algorithm 1**   
Receive Packet from MAC

|  |
| --- |
| **Inputs:** received packet, *P*, current time, *t*, received packet cache, *C*, forwarding queue, *Q*, current node depth, *D*, and threshold for minimum depth advantage, *dmin*. **Outputs:** Updated cache, *C*, and forwarding queue, *Q*.  Procedure:  *d* ←*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*   ′ ←*Q.get*(*P.srcID, P.seqNo*) ⊳ *obtain the old packet P*   **if** *d > dmin* ⊳ *if depth gain above the threshold*   *tH*←*calculateHoldingTime*(*d*) ⊳ *using equation* (1)   *tF*←*t* + *tH* ⊳ calculate the forwarding time   **if** *P*′ *.timer.expires > tF* ⊳ if the forwarding time is sooner than old forwarding time  *P*′ *.timer.expires*←*tF* ⊳ 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*←**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 > dmin* ⊳ if depth gain above the threshold   *tH*←calculateHoldingTime(*d*) ⊳ using equation (1)   *tF*←*t* + *tH* ⊳ calculate the forwarding time   *P.depth*←*D* ⊳ update the packet depth   *P.dropFlag*←**false** ⊳ do not drop the packet yet |

(*continued on next column*)

4

*A. Alharbi et al.*  *Array 13 (2022) 100117*



**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* un-qualified neighbors holding a copy of the same packet, then the expected number of additional forwarded packets is (*p* ⋅*m*) packet. Unqualified forwarding neighbors is a subset of all neighbors within a node’s communication range. Obviously, neighbors that have already for-warded a specific packet are no longer considered unqualified for-warders 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. There-fore, the overhead caused by probabilistic forwarding is expected to be reasonably low.

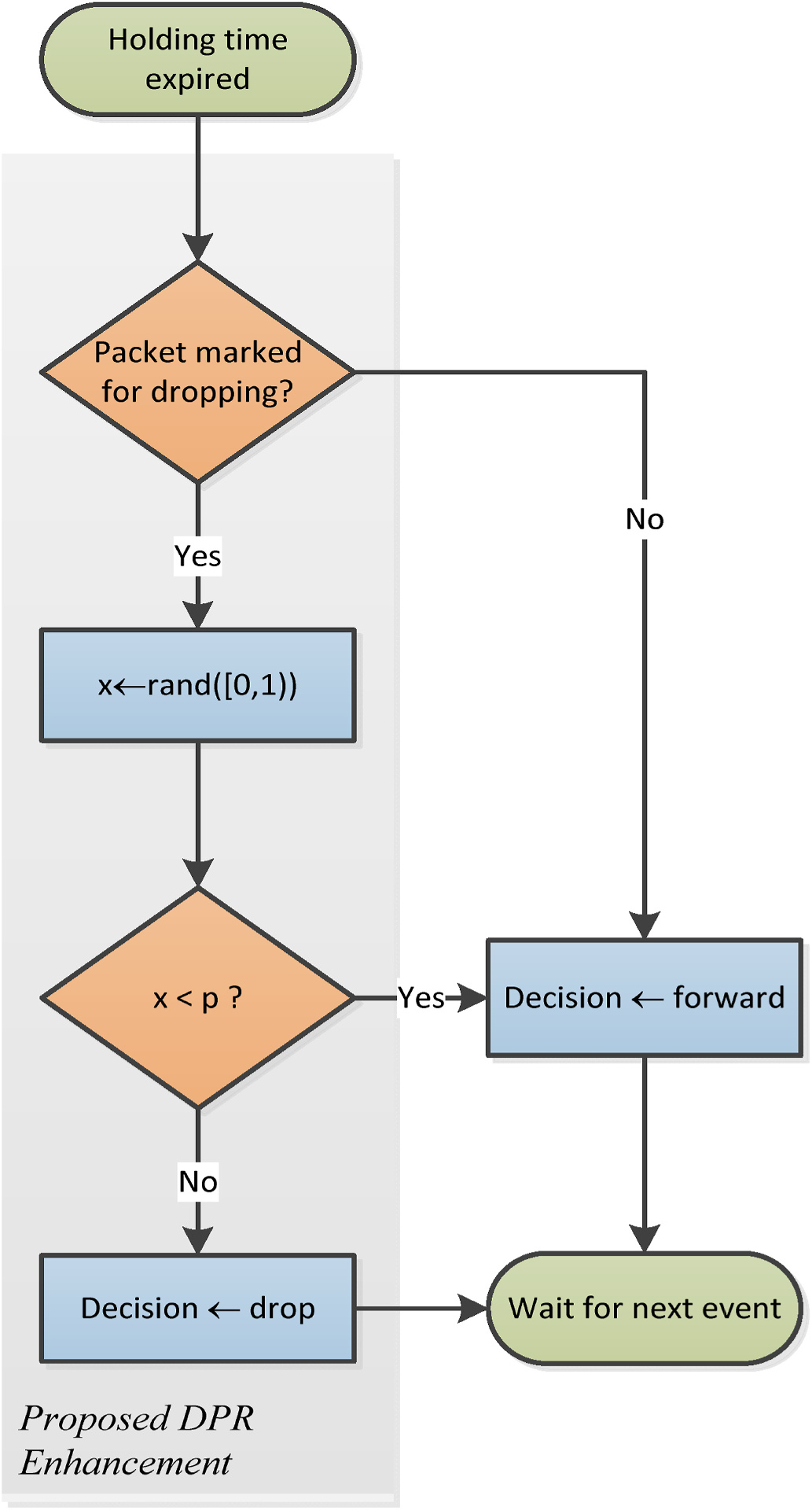
To sum up the effect of the probability parameter *p*, there seems to be a trade-off between the achievable delivery ratio and the overhead due to the additional packets forwarded. It is expected that a large *p* im-proves delivery ratio when the network is under a depth-spoofing attack but also increases 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 simu-late it with various values of *p* for each of the two cases: with attack and without attack. Two metrics are calculated—the delivery ratio *rp*, and overhead, *wp*—corresponding to each value of *p*. The delivery ratio *rp* for a given forwarding probability *p* is calculated as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| *r* | *D*′  *p* | (2) | |
| *p* = | *D*0 |
| 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 equiv-alent to the behavior of the original DBR. The overhead, *wp*, is calculated as follows: | | | |
| *wp* =*Fp* | | *,* | (3) |

where *Fp* is the total number of packets transmitted by all the nodes

5

*A. Alharbi et al.*  *Array 13 (2022) 100117*



**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*κ*log 10(*d*) + *d* × 10−3*α*(*f*) (5)

where *f* is the center frequency in kHz, A0 = 30 *dB* is a normalizing constant, *κ* is the spreading factor, *d* is the distance in meters and *a* is the

6

*A. Alharbi et al.*  *Array 13 (2022) 100117*

**Table 1**   
Simulation settings.

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

absorption coefficient, which is further defined as follows:

|  |  |  |
| --- | --- | --- |
| *α*(*f*) =0*.*11*f* 2 1 + *f*2 + | 4100 + *f*2 + 2*.*75 × 10−4*f* 2 + 0*.*003 dB 44*f*2 / km | (6) |
| We simulated the spherical spreading by setting the spreading factor *κ* = 2 in Equation (5). The ambient noise can be approximated by the following power spectral density: | | |
| *N*(*f*) = 50 − 18log 10(*f*) | | (7) |
| The signal-to-noise ratio can be calculated using the following formula: | | |

*γ*(*f*) = *SL* − *N*(*f*) − *A*(*f*)

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

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 pres-ence of an active attacker and observed the packet delivery ratio *rp* 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* ≥ 0*.*9, *p* ≥ 0*.*7 and *p* ≥ 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 prob-ability needed to achieve a certain delivery ratio.

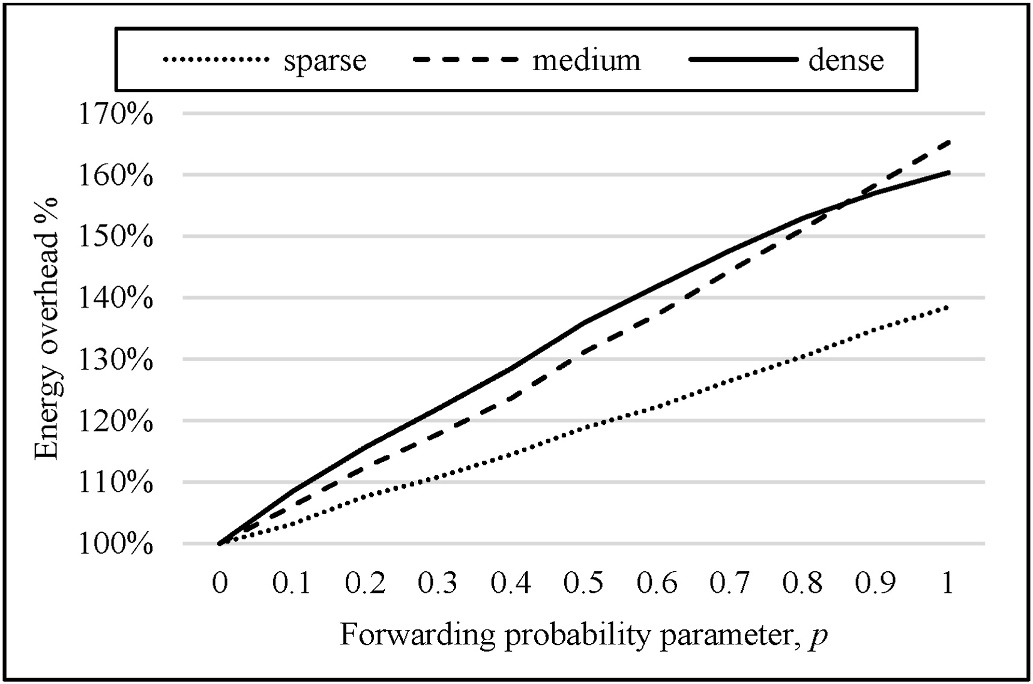
*Pt* = 2*π zd* × 0*.*67 × 10−18× 100*.*1 *SL*  *5.2. DPR overhead*

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

|  |
| --- |
| *ε* =1 2⎛⎝1 −√̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅̅1 + 100*.*1 *γ*(*f*)⎞⎠ (8)  Therefore, the probability of successful reception of a packet of length *m* bits is (1 − *ε*)*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 pro-tocols 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, *rp*, 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 |

7

*A. Alharbi et al.*  *Array 13 (2022) 100117*

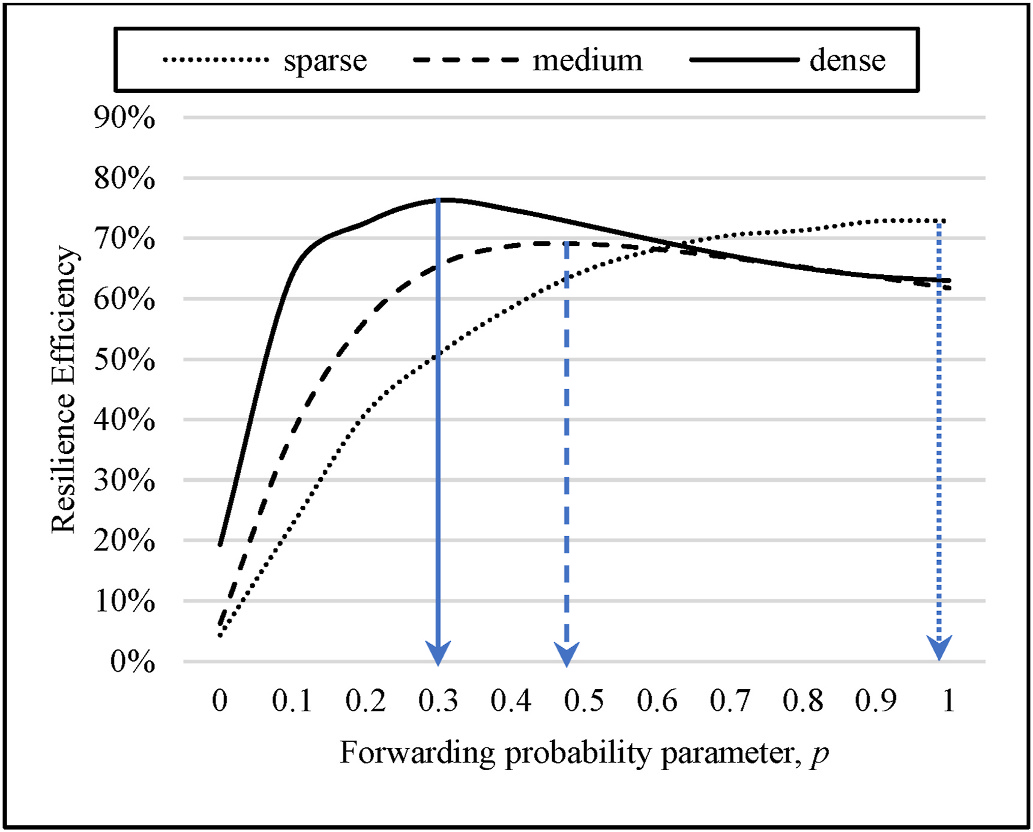


**Fig. 6.** Effect of forwarding probability on delivery cost in the absence of depth-spoofing attack, with varying node densities.

*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).

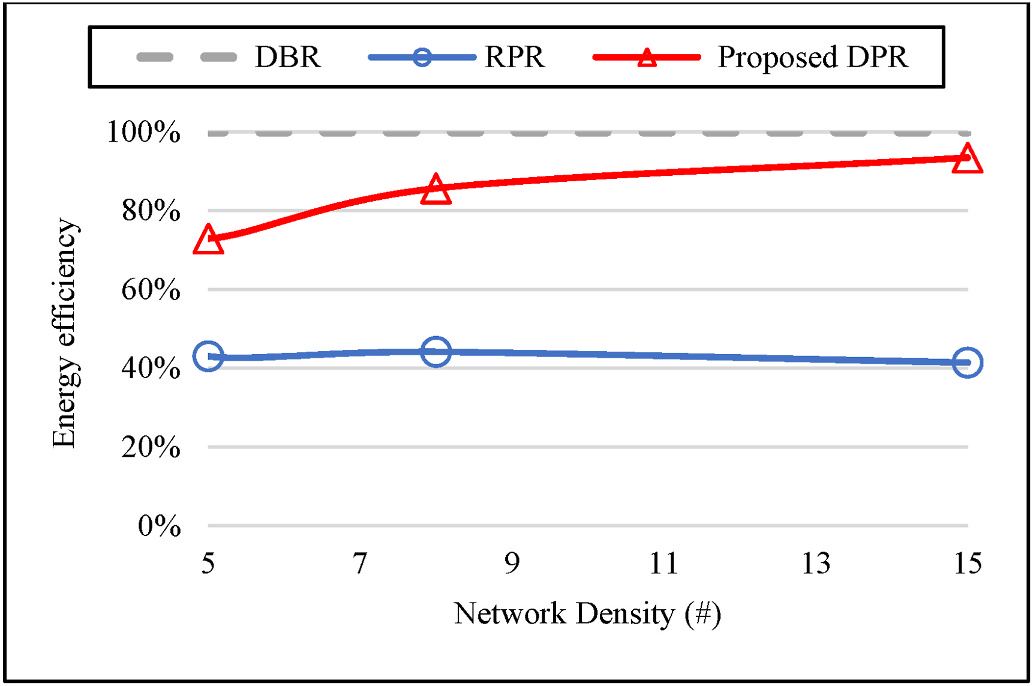
Fig. 7 illustrates how the optimal resilience efficiency is affected by the network density. In the sparse network, where the overhead is significantly limited, it seems that the delivery ratio is the overwhelming factor affecting resilience efficiency. Therefore, the best resilience effi-ciency was 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*.



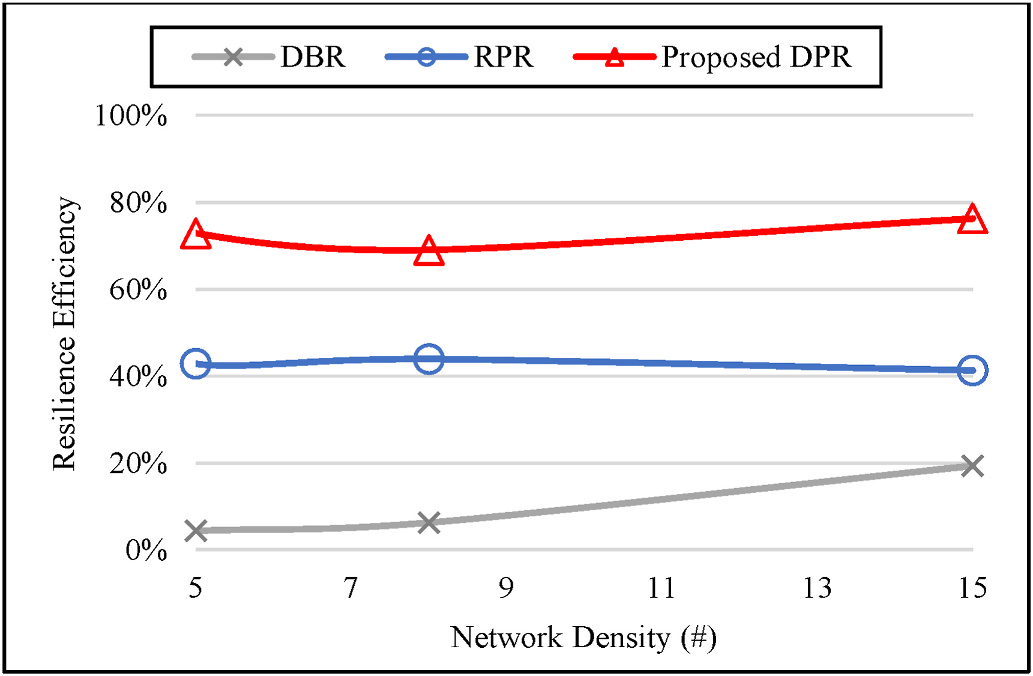
**Fig. 7.** Finding the optimal forwarding probability using the resilience effi-ciency, ***η***. In the sparse network (a), the maximum ***η*** is at ***p*** = 0.9. In the medium-density network (b), the maximum ***η*** is at ***p*** = 0.5. In the dense network (c), the maximum ***η*** is at ***p***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

8

*A. Alharbi et al.*  *Array 13 (2022) 100117*



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



**Fig. 9.** Comparison of resilience efficiency.

*Node depletion rate* =*Numberof node transmissions*

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 for-warding. The simulation showed that the proposed DPR protocol is potent against depth-spoofing sinkhole attacks. Since energy consump-tion 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

9

*A. Alharbi et al.*  *Array 13 (2022) 100117*

**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://](https://doi.org/10.1016/j.procs.2019.01.225) [doi.org/10.1016/j.procs.2019.01.225](https://doi.org/10.1016/j.procs.2019.01.225).

[2] [T. Dargahi, H. H. S. Javadi, and H. S](https://doi.org/10.1016/j.procs.2019.01.225)hafiei, "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.](https://doi.org/10.1145/3366486.3366546) [org/10.1145/3366486.3366546](https://doi.org/10.1145/3366486.3366546) [Online]. Available:.

[4] [Jiang S. On securing underwate](https://doi.org/10.1145/3366486.3366546)r acoustic networks: a survey. IEEE Communications Surveys & Tutorials 2019;21(1):729–52. [https://doi.org/](https://doi.org/10.1109/COMST.2018.2864127) [10.1109/COMST.2018.2864127](https://doi.org/10.1109/COMST.2018.2864127).

[5] [Yan H, Shi Z, Cui J-H. DBR: depth-based routing for underwater sensor networks.](http://refhub.elsevier.com/S2590-0056(21)00055-2/sref5)

[In: NETWORKING 2008 ad hoc and sensor networks, wireless networks, next](http://refhub.elsevier.com/S2590-0056(21)00055-2/sref5) [generation internet, vol. 4982. Berlin, Heidelberg: Springer Berlin Heidelberg;](http://refhub.elsevier.com/S2590-0056(21)00055-2/sref5) [2008. p. 72–86 (Lecture Notes in Computer Science.](http://refhub.elsevier.com/S2590-0056(21)00055-2/sref5)

[6] [Yu H, Yao N, Wang T, Li G, Gao Z, Tan G. WDFAD-](http://refhub.elsevier.com/S2590-0056(21)00055-2/sref5)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,](https://doi.org/10.1016/j.adhoc.2015.08.023) 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, "](https://doi.org/10.1155/2014/213012)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://ieeex[plore.ieee.org/document/7289175.](https://doi.org/10.1109/IWCMC.2015.7289175)

[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.](https://doi.org/10.1109/ICACS.2018.8333483)

[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.](https://doi.org/10.1109/ICOSST.2016.7838592)

[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](https://doi.org/10.1007/s10772-020-09700-3) 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/Confluence47617.2020.905798](https://doi.org/10.1109/Confluence47617.2020.9057981)1.

[14] Zuba M, F[agan M, Jun-Hong C, Zhijie S. A vulnerability study of ge](https://doi.org/10.1109/Confluence47617.2020.9057981)ographic 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://ieeex[plore.ieee.org/document/6682698.](https://doi.org/10.1109/CNS.2013.6682698)

10