DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks

Ayman Alharbi
Department of Computer Engineering
Collage of Computer Science and Information Systems
Umm Al-Qura University, Mecca
Saudi Arabia

***Abstract*—Depth-Based protocol has gained considerable attention as an efficient routing scheme for Underwater Wireless Sensor Networks UWSNs. It requires only depth information to perform the routing process. Despite this feature, UWSNs which operate with the employment of DBR protocol are vulnerable to depth spoofing attack. In this paper, Depth Based Secure Routing protocol is proposed to overcome this vulnerability. DBSR modifies traditional DBR routing algorithm by securing the depth information which is embedded in the header part of DBR packet. In addition to that, each node verifies the sender's identity based on a digital signature scheme. We extensively evaluate the overhead and performance gain of DBSR for two signature schemes based on Elliptic Curve Cryptography method considering various network conditions. The simulation study is performed using NS3-based simulator. Our results show that DBSR can avoid depth-spoofing attack by achieving 95% and 85% delivery ratios under low and high network loads respectively. Contrary to popular belief, results show that careful utilization of cryptographic techniques is justifiable without significant overhead on the communication cost.**

***Keywords*—UWSN; DBR; ECC**

I. INTRODUCTION

Water covers more than 70% of earth planet. The nature of underwater world includes valuable resources such as unique minerals, various food sources, and other undiscovered sites. Traditionally, a diver or marine underwater vehicle collect data from fixed sensors which were used in order to observe underwater information. However, due to the harsh and unsafe environment of underwater world, scientists continue developing more tools to be used remotely [1], [2] . Moreover, this approach is not suitable for real-time applications such as military surveillances. As a result, Underwater Wireless Sensor Networks (UWSNs) have emerged as a promising technology due to their unique features [3] [4] [5]. First, underwater sensor networks provide useful sensing capabilities that can be used for long-term and short-term monitoring. They have the capability to be operated days, weeks, months even years wirelessly, hence, enable of wide sensing fields such as: temperature, salinity, current movements, video, image, chemical sensing [6][7]. Second, high density feature allows extensive discovering and exploration of wide underwater areas. Third, real-time sensing and monitoring missions can be achieved using underwater sensor networks [8]. Fourth, when unexpected failure occurred in any sensor in the network, rapid error detection and remote fixing are applicable features using underwater sensor networks [9]. Fifth, compared to traditional underwater equipment, underwater sensor networks offer the possibility of re-configuring sensors remotely and eliminate the need for physically accessing underwater sites. In summary, UWSNs help to transmit data through wide distances and harsh circumstances. Figure 1 shows an example of UWSN architecture. In this architecture, each underwater node is capable of gathering, relaying data through different transmission media (acoustic or optical) waves to the surface gateway. After collecting data from underwater nodes, gateways nodes transmit the observed data to the base station using radio waves.

There has been considerable effort to enhance the performance of UWSN for different objectives e.g. delay, power, mobility and other performance goals [10], [11]. Depth based routing protocol [12] was proposed in order to enhance routing functionality of UWSNs. In this protocol, the forwarding procedure depends mainly on the depth information of the source of each received packet. In other word, the main advantage of DBR is that it free doesn't depend on complex geographic computation and perform a free localization method. In traditional DBR protocol, the routing mechanism is based on depth information of each forwarder node. When the node receive a packet, it checks the forwarder/sender depth then check if it is candidate for forwarding the received packet. If the sender's depth is larger than its depth, it hold the packet for a certain amount of time called "holding time". If this condition is not met, the packet will immediately be dropped. However, this approach is vulnerable to serious security attack namely, depth-spoofing attack [13]. In this attack, sender's depth could be compromised and utilized for malicious activities. If an adversary succeeded in gaining information about current topology, it can easily deploy a malicious node at an excellent location where it can receive packets form different nodes in the network. In this case, the attacker will forward that packet with a fake depth projecting a better position. Accordingly, any node located at the attacker's transmission range will drop their packets after receiving attacker's spoofed message.

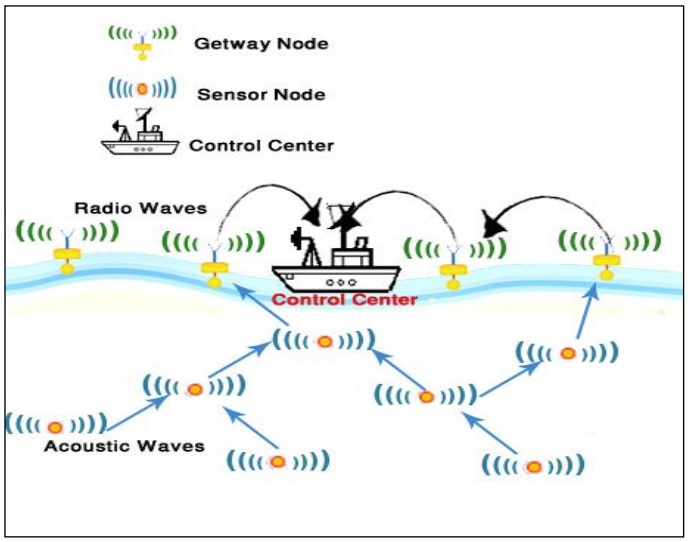

Fig. 1. UWSN Architecture.

In this paper, we propose Depth Based Secure Routing protocol to mitigate the abovementioned vulnerability. We seek to study the performance analysis of securing DBR protocol based on cryptography approach extensively. The performance analysis considers state-of-the-art encryption schemes designated energy-constrained devices.

The rest of the paper is organized as follows: Section II points out relevant background and details the attack model. In Section III, related work is reviewed. Section V presents the proposed solution. Section VIVI highlights the main findings based on simulation results. Finally, Section VII summarize author's conclusions.

II. Background

Due to the unique challenges of aquatic environment, proactive or reactive general routing protocols do not behave well underwater and considered very costly. Hence, Geographic routing protocols provides better performance and most suitable for UWSN's.

A. Geographic Information-based Routing

Geographic routing protocols depend on location information of sensor nodes. The key factor of establishing routing paths between the source and destination is the location of each node. VBF [14] and DBR [12] are both among the most common geographic information-based routing protocols which are built for UWSNs. In this subsection, we review the main functionality of the two protocols. However, the main focus will be on DBR to highlight recent enhancements to this protocol, and its existing vulnerability named as the depth spoofing attack.

1) Vector Based Forwarding (VBF) Routing: In VBF, a path form source to destination will be limited to only few number of nodes which satisfy certain geographic conditions. Therefore, the vector allow will only high benefit nodes to be participated in the forward process. Other nodes will discard the packets to save energy. As it mentioned, participation in routing depends on which nodes fall in the path between source and destination. The packet compose of three fields, the sender (A), the sink (B), and the forwarder. The algorithm will find the routing vector from the sender to the sink A to B, then forward packets along the path. Each node belong to the path can forward the packets based on calculating a specific factor. This factor is called the "desirableness factor" which determines the suitableness of each candidate forwarding node. As a result, the node will discard if the calculated factor is large. Accordingly, if the results is 0, it will be optimal node for forwarding the packet.

2) Depth Based Routing Protocol DBR: The basic idea behind DBR is that, a node need only the recognize sender's depth to decide whether it is eligible to forward the received packet or drop it. Hence, only optimal forwarder nodes will be considered among the routing process. Therefore, one of the main advantages of DBR is that any node inside the network doesn't need to have any information about the current topology or further locations information of other nodes.

Among the preparation process of the transmission of a generated packet, an important step which the source node incorporates its depth in the header part. While all nodes which are located at the same transmission range of the sender will receive the packet, a packet will be dropped if the sender's depth d_s is lower than the receiving node's depth dr. Consequently, if $ds > dr$ receiving node will be candidate to forward the packet.

It is worth mentioning that candidate node will keep the received packet for a certain period of time called "holding time (T)". This factor is used for the advantage of calculating the closest node to the surface which will be the qualified forwarder for the packet. The holding time cab be calculated as :

$$T = K(Y - \delta) \quad (1)$$

where Y is the communication range for the node and δ is the difference between d_s and d_r. K is a constant which can be used to determine the maximum holding time.

a) DBR enhancement: Energy-Efficient Depth-Based Routing EEDBR protocol was proposed by [15] . The key difference between DBR and EEDBR is the decision of selecting the forward node. In EEDBR, the decision will be based on both the depth and the residual energy of the forwarder. The protocols requires that each node will broadcast its residual energy and depth to its neighbors frequently. Unfortunately, this drawback add more overhead to the routing procedure since more packets are required.

Light-weight depth-based routing LDBR was also proposed to enhance DBR for underwater wireless sensor network [16]. As in EEDBR, the residual energy is also taken into consideration when candidate nodes receive packets from the sender. However, the enhancement was made to the decision of determining the optimal forwarder. In addition of depth condition, the residual energy of sender and next hop packet will be one of the main factors to determine the optimal forwarder node.

An Improved Adaptive Mobility of Courier Nodes in Threshold-Optimized BDR Protocol IAMCTD was proposed [17]. In this proposed approach, the authors designed an improved DBR protocol to deal with real-time sensitive applications. In addition of depth, other network parameters also considered for routing decision such as network density. The protocol improved the network lifetime as well as transmission loss.

An Optimized Depth-Based Routing Protocol for Underwater Wireless Sensor Networks ODBR was also proposed [18]. The protocol address a shortcoming point which exists in DBR protocol. The nodes closest to the sink will lose energy more than other network nodes. Therefore, the proposed algorithm ensured an optimized method for energy balancing between all nodes. In ODBR, nodes with high traffic will be marked for a specific zone in order to reduce the energy consumption. Hence, ODBR improves lifetime, throughput and energy consumption of UWSNs.

III. Related Work

Authors in [19] presented a study for evaluating the cost of digital signature schemes. They highlighted the usability of applying digital signature schemes for the environment of UWSNs. However, the study only considered the cost of signing while the verification cost is assumed to be performed by the sink only. Moreover, the routing protocol is not specified. In [20], authors mitigated the effect of depth-spoofing attack by combining between authentication-based method and thresholding strategy. Unlike DBR protocol, node will compare its depth with lower/upper bounds threshold. Hence, if the receiver's depth falls within range of threshold, it forwards the packet. This window is calculated randomly by the sender depending on its neighbors information. However, the proposed approach suffered high transmission cost since each source node will depend on a randomized threshold window which may rise the cost significantly.

IV. Attack Model

We adapt the attack model presented in [6] to validate our proposed solution. In this attack model, the attacker first will try to eavesdrop the transmission and listen to at least two nodes in the area. Figure 2 illustrates the attack strategy. The source S is in the same range of first forwarder node f1. The attacker is also able to hear transmissions generated by the source because it is located in the same transmission range. When the source transmit packet, f1 should compare its depth with the source's one. F1 will decide to hold the packet for a certain threshold since its depth is the lower than the source The packet should be forwarded by f1 to f2 by the end of holding time, however, since the attacking node received the same packet, it forward it with spoofed depth assuming lower value than f1. Accordingly, f1 will drop the packet which has been delayed due to the holding time period. Consequently, all other nodes in the attacker transmission range will receive the same packet with smaller depth and then will drop their packet. As a result, the attacker is network.

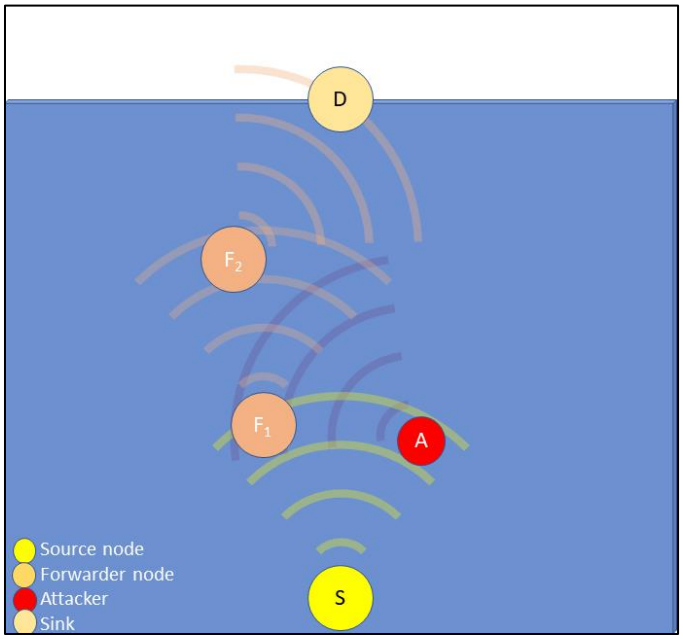

Fig. 2. Depth-Spoofing Attack.

V. Proposed Method

A. Justifications

- Our proposed method is based on light cryptography techniques using elliptic curve algorithm which utilize fewer bits to secure transmission.
- The proposed method secure DBR routing protocol one of the most widely used in the are of underwater sensor networks.
- There is lack of extensive performance analysis of utilizing cryptography techniques to secure DBR protocol.

B. Assumptions

- The attacker and the legitimate nodes have the same transmission range.
- The attacker has better capability so that he/she will choose the best location in the network based on many factors such as (depth, weak links .. etc.).
- We assume homogeneous nodes i.e. all nodes have the same level of energy.
- We ignore the computation cost since it is negligible to communication cost for UWSNs [20].
- All public/private keys inside each node are secured by strong hardware-rooted encryption platform that makes it infeasible to compromise a node.
- We assumes that no additional nodes will be added to the network. Therefore, we leave the scalability issue for future work.

Able to prevent further transmissions and crash the DBSR methodology.

To mitigate the effect of depth spoofing attack we need to protect that sensitive information on which the best forwarder for the packet is selected. As depicted in Figure 3 DBR protocol encapsulates the sender's depth with each packet as a part of the header. Unquestionably, this tiny information is very sensitive and it is highly vulnerable to the depth-spoofing attack. Our proposed approach add the following additional security steps to the existing protocol:

1) Pair of security keys (private/public) will be assigned to each node before deployment. The private key will be used for signing whereas the public key used for verification.

2) Each sensor node will be configured with its own private key and a list of all public keys of other node.

3) Pair of security keys (private/public) will be assigned to each node before deployment. The private key will be used for signing whereas the public key used for verification.

4) Each sensor node will be configured with its own private key and a list of all public keys of other nodes.

5) The DBSR packet header, shown in shown in Figure 3 contains two additional fields: The recent forwarder ID and the forwarder signature.

6) The sender/forwarder calculates the signature of: Packet ID (source ID , sequence number), forwarder ID, and forwarder depth.

7) The sender/forwarder places its signature and then transmits the whole packet to the next hop.

8) A receiver first verifies the signature. If the verification fails, the packet is considered malicious and it will be ignored.

Figure 4 summarizes the steps of the DBSR protocol. In the deployment stage, each node will be configured with pair of public/private key. In addition, each node stores list of all public keys of other nodes. In the operation stage, each node will verify sender's depth before accepting the received packet.

C. Proposed Signature Scheme

UWSNs have unique characteristics which restrict the available resources for cryptography operations. Due to the limitation of available energy at underwater wireless nodes, ECC-based schemes are considered more suitable for wireless devices [19]. Therefore, we consider two efficient ECC-based algorithms for DBSR design, ECDSA and BLS digital signatures methods. As can be depicted from algorithm 1, the signing process leads to additional bits, therefore, the overhead will be investigated per hop considering various network conditions.

VI. Performance Analysis

A. Expirement Settings

To evaluate the overhead of authentication on the network, we set up three scenarios as follow: First, we highlight the behavior of DBR under different network conditions and various message lengths. Second, we investigate the effect of depth-spoofing attack on DBR. Third, we study the overhead of DBSR considering two encryption schemes.

Throughout the experiment, to study the effect of network capacity, we run the simulation for different generation bit rate of source nodes, namely 10 b/s, 50 b/s and 100 b/s for light, medium and high loads, respectively. Also, for effect of message length, we interchange the value of message length between 100b and 1kb. Moreover, we investigate the effect of attacker capability by varying number of malicious nodes between 1 and 7 nodes. Finally, for the effect of different signature schemes, we interchange the overhead between 40 bits and 20 bits for ECDSA and BLS respectively. Other simulations settings can be summarized in Table I.

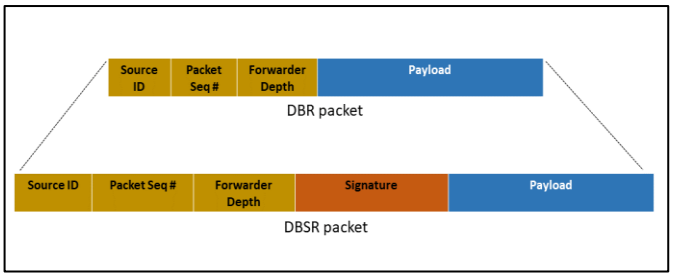

Fig. 3. DBR and DBSR Packet Format.

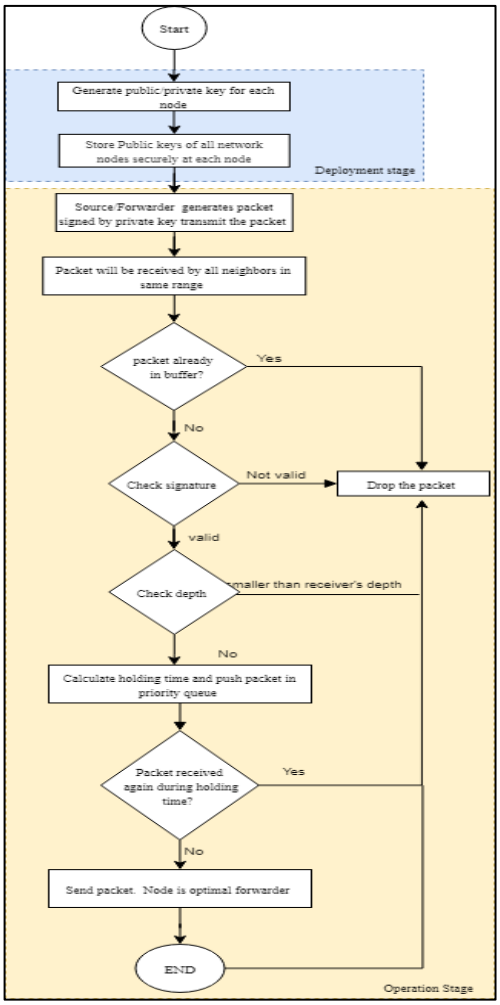

Fig. 4. DBSR Flowchart.

Algorithm 1 DBSR sender signature generation based on ECDSA

1. **Compute** the header hash **h** = hash(**header**)
2. **Compute** a random number **k** where $1 \leq \mathbf{k} \leq (p-1)$
3. **Compute** random point (**x1**, **y1**) = **k** × Base point(x,y) mod **p**
   r = **x1** mod **n**
4. **Check r** $\neq 0$, if yes then **repeat** steps 1to 3
5. **Compute** signature **S** = ($\mathbf{k}^{-1}$ (**h** + **sender's private key** × **r**)) $mod\ n$

Algorithm 2 DBSR signature verification by receiver based on ECDSA

1. **Compute w** = $\mathbf{S}^{-1}$ mod **n**
2. **Compute u1** = (**h**×**w**) mod **n**
   u2 = (**r**×**w**) mod **n**
3. **Compute C(x2,y2)** = **u1**× Base point(x,y) + **u2** × **sender's public key**
4. **Check x2 (mod p)** $\neq$ **r,** if yes **reject and report to sink**

TABLE I. SIMULATION PARAMETRES

Parameter	Value
Network area	$500m \times 500\ m$
Network Density	3
Number of source nodes	7
Communication Ranges	150 m
Interference Ranges	300 m
Interference Range	300 m
Total number of nodes	30 nodes
Channel Bit Rate	10000 b/s
ECDSA signature size	40 bits
BLS signature size	20 bits

B. DBSR vs DBR

To show the effectiveness and benefits of DBSR, we compare the delivery ratio and packet loss percentage of DBR protocol with DSBR protocol under low, medium and high traffic loads.

As can be observed from Figure 5 and Figure 6, DBR will be significantly affected by active attack especially when the networks operates under low traffic. The number of delivered packets decreases from 600 to 50 packets. On the other hand, DBSR improved the performance by achieving 585 successfully delivered packets.

C. Effect of Attacker Capability

Unquestionably, when the number of attacking nodes increases, the chance of attack effect increases. As can be seen in Figure 7 and Figure 8, the effect of the number of attackers on the delivery ratio is dominant. The more attacked nodes, the lower the delivery ratio. In the worst case, the attackers can reduce the delivery ratio by 91%. Similarly, the more attacked nodes, the higher the packet loss ratio. In the worst case, the attackers can increase the packet loss ratio by 90%. As can be observed also, the effect of the attack is more severe in lightly loaded networks. In addition, it is worth mentioning that when the network operates under no attack, the main factor affecting delivery ratio is the network load. Delivery ratio in a highly loaded network can be as low as 36% as can be seen in Figure 8.

D. Effect of Message Length

As mentioned previously, we evaluate the effect of different message lengths by considering small a long values for each generated message. As can be depicted by Figure 8, the effect of message length is negligible especially in lightly loaded networks (<2% change in delivery ratio). This is encouraging because it indicates that adding authentication can be justified in lightly loaded network.

E. Effect of Authentication

As can be seen in Figure 9, the overhead of authentication is smaller for long messages. Same results show that overhead of BLS authentication is smaller than ECDSR. This is due to the fact that BLS generates shorter signatures than ECDSR. The difference between BLS and ECDSA is more significant for the case of short messages in a highly loaded networks. This is due to the fact the overhead of authentication almost doubles the network load which leads to excessive packet loss due to congestion.

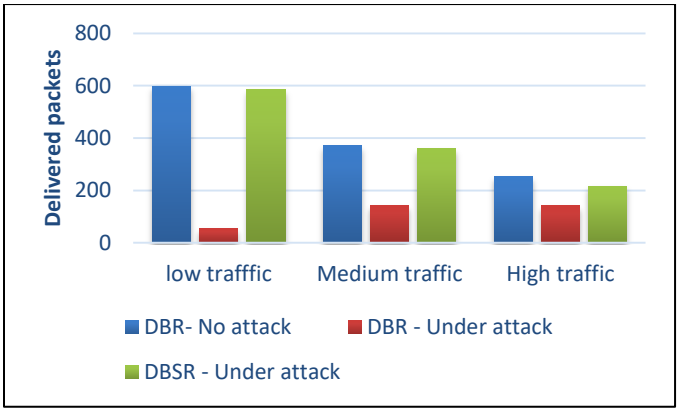

Fig. 5. DBR vs DBSR Delivered Packets.

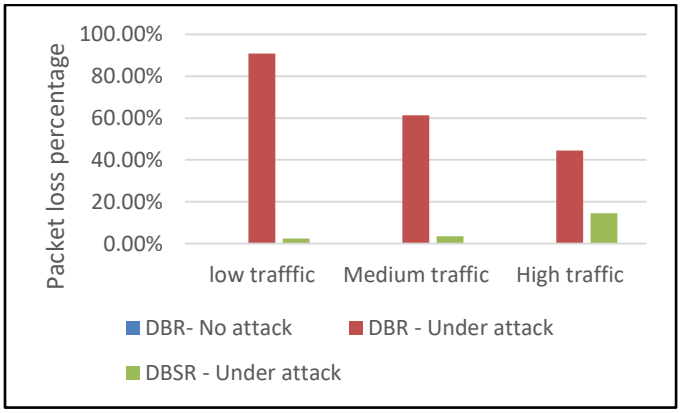

Fig. 6. DBR VS DBSR Packet Loss.

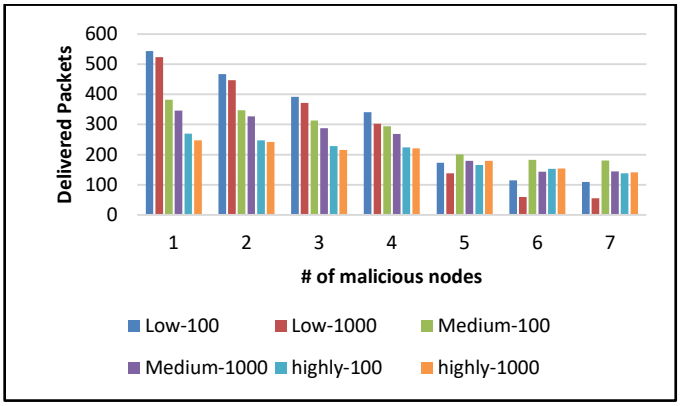

Fig. 7. FEffect of Attacker Capability.

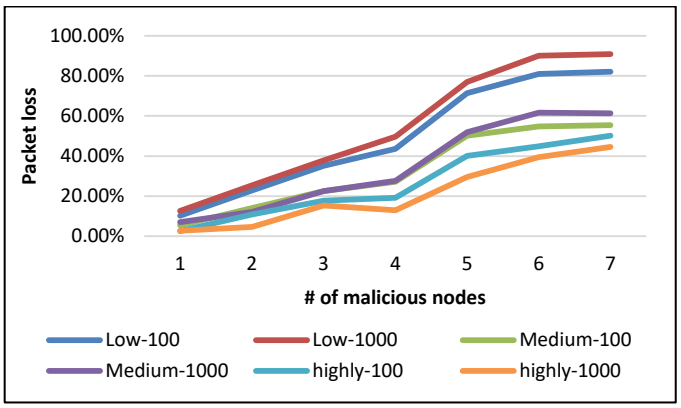

Fig. 8. Effect of Message Lengths.

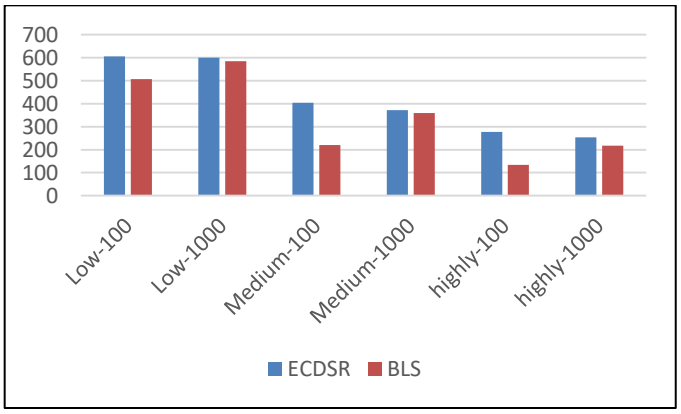

Fig. 9. ECDSA Vs BLS.

VII. Conclusion and Futre Work

In this paper, a security improvement to DBR routing protocol based on ECC scheme was introduced. The proposed approach eliminates depth-spoofing attack by securing the depth information. The proposed method suggests the use of an encryption mechanism, namely ECC algorithm. The key contribution is the study of signature overhead considering various network parameters. Simulation results show that the proposed scheme archives high delivery ratio. Results also show that there is high dependency between certain network parameters such as: network load and packet nominal length on one hand and signature overhead on the other hand. Our future work to extend the proposed approach to allow key exchange an interesting question that arose from this research is how to enhance this approach so a new node can be added to the network without need for mutual authentication between nodes.

Acknowledgment

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code 19-COM-1-01-0019.

References

[1] J. Watt, M. R. Phillips, C. E. A. Campbell, I. Wells, and S. Hole, “Wireless Sensor Networks for monitoring underwater sediment transport,” Science of the Total Environment, vol. 667. Elsevier B.V., pp. 160–165, Jun. 01, 2019, doi: 10.1016/j.scitotenv.2019.02.369.

[2] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, “Challenges and Security Issues in Underwater Wireless Sensor Networks,” in Procedia Computer Science, 2019, vol. 147, pp. 210–216, doi: 10.1016/j.procs.2019.01.225.

[3] I. F. Akyildiz, D. Pompili, and T. Melodia, “Underwater acoustic sensor networks: Research challenges,” Ad Hoc Networks, vol. 3, no. 3, pp. 257–279, May 2005, doi: 10.1016/j.adhoc.2005.01.004.

[4] A. A. Sheikh, E. Felemban, M. Felemban, and S. B. Qaisar, “Challenges and opportunities for underwater sensor networks,” in Proceedings of the 2016 12th International Conference on Innovations in Information Technology, IIT 2016, Mar. 2017, doi: 10.1109/INNOVATIONS.2016.7880021.

[5] H. Alhumyani, R. Ammar, H. Albarakati, and A. Alharbi, “Deployment strategies for underwater sensing and processing networks,” in Proceedings - IEEE Symposium on Computers and Communications, Aug. 2016, vol. 2016-August, pp. 358–363, doi: 10.1109/ISCC.2016.7543766.

[6] R. W. L. Coutinho, A. Boukerche, L. F. M. Vieira, and A. A. F. Loureiro, “Underwater Sensor Networks for Smart Disaster Management,” IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 107–114, Mar. 2020, doi: 10.1109/MCE.2019.2953686.

[7] M. Jouhari, K. Ibrahimi, H. Tembine, and J. Ben-Othman, “Underwater Wireless Sensor Networks: A Survey on Enabling Technologies, Localization Protocols, and Internet of Underwater Things,” IEEE Access, vol. 7, pp. 96879–96899, 2019, doi: 10.1109/ACCESS.2019.2928876.

[8] N. Javaid, U. Shakeel, A. Ahmad, N. Alrajeh, Z. A. Khan, and N. Guizani, “DRADS: depth and reliability aware delay sensitive cooperative routing for underwater wireless sensor networks,” Wireless Networks, vol. 25, no. 2, pp. 777–789, Feb. 2019, doi: 10.1007/s11276-017-1591-1.

[9] G. Han, X. Long, C. Zhu, M. Guizani, and W. Zhang, “A High-Availability Data Collection Scheme based on Multi-AUVs for Underwater Sensor Networks,” IEEE Transactions on Mobile Computing, vol. 19, no. 5, pp. 1010–1022, May 2020, doi: 10.1109/TMC.2019.2907854.

[10] N. Li, J.-F. Martínez, J. Meneses Chaus, and M. Eckert, “A Survey on Underwater Acoustic Sensor Network Routing Protocols,” Sensors, vol. 16, no. 3, p. 414, Mar. 2016, doi: 10.3390/s16030414.

[11] S. Sahana, K. Singh, R. Kumar, and S. Das, “A review of underwater wireless sensor network routing protocols and challenges,” in Advances in Intelligent Systems and Computing, 2018, vol. 638, pp. 505–512, doi: 10.1007/978-981-10-6005-2_51.

[12] H. Yan, Z. J. Shi, and J. H. Cui, “DBR: Depth-based routing for underwater sensor networks,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008, vol. 4982 LNCS, pp. 72–86, doi: 10.1007/978-3-540-79549-0_7.

[13] M. Zuba, M. Fagan, J. H. Cui, and Z. Shi, “A vulnerability study of geographic routing in underwater acoustic networks,” in 2013 IEEE Conference on Communications and Network Security, CNS 2013, 2013, pp. 109–117, doi: 10.1109/CNS.2013.6682698.

[14] P. Xie, J. H. Cui, and L. Lao, "VBF: Vector-based forwarding protocol for underwater sensor networks," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2006, vol. 3976 LNCS, pp. 1216–1221, doi: 10.1007/11753810_111.

[15] A. Wahid, S. Lee, H. J. Jeong, and D. Kim, "EEDBR: Energy-efficient depth-based routing protocol for underwater wireless sensor networks," in Communications in Computer and Information Science, 2011, vol. 195 CCIS, pp. 223–234, doi: 10.1007/978-3-642-24267-0_27.

[16] S. Gul, S. H. Jokhio, and I. A. Jokhio, "Light-weight depth-based routing for underwater wireless sensor network," in 2018 International Conference on Advancements in Computational Sciences, ICACS 2018, Apr. 2018, vol. 2018-January, pp. 1–7, doi: 10.1109/ICACS.2018.8333483.

[17] N. Javaid, M. R. Jafri, Z. A. Khan, U. Qasim, T. A. Alghamdi, and M. Ali, "IAMCTD: Improved adaptive mobility of courier nodes in threshold-optimized DBR protocol for underwater wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 2014, Nov. 2014, doi: 10.1155/2014/213012.

[18] T. Ahmed, M. Chaudhary, M. Kaleem, and S. Nazir, "Optimized depth-based routing protocol for underwater wireless sensor networks," in ICOSST 2016 - 2016 International Conference on Open Source Systems and Technologies, Proceedings, Jan. 2017, pp. 147–150, doi: 10.1109/ICOSST.2016.7838592.

[19] E. Souza, H. C. Wong, I. Cunha, A. A. F. Loureiro, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in under-water sensor networks," in Proceedings - International Symposium on Computers and Communications, 2013, pp. 299–304, doi: 10.1109/ISCC.2013.6754963.

[20] M. Zuba, M. Fagan, Z. Shi, and J. H. Cui, "A resilient pressure routing scheme for underwater acoustic networks," in 2014 IEEE Global Communications Conference, GLOBECOM 2014, Feb. 2014, pp. 637–642, doi: 10.1109/GLOCOM.2014.7036879.