Jestr

Journal of Engineering Science and Technology Review 11 (5) (2018) 10 - 16

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Secure Robust Pressure based Routing for Underwater Acoustic Sensor Network

R. Bhairavi* and Gnanou Florence Sudha

Department of Electronics and Communication Engineering, Pondicherry Engineering College- Puducherry - 605014, India.

Received 12 September 2018; Accepted 23 October 2018

Abstract

The distinctive characteristics of Underwater Acoustic Sensor network, makes it highly susceptible to attacks. Effective and skilful interaction between the sensors and Autonomous Underwater Vehicles is required to actuate the communication in the network. In the existence of malicious nodes, this leads to critical security issues especially in pressure based routing protocols. Thus, an effective security scheme is indispensable for efficient data transmission. In this paper, the prime aim is to detect the virulent nodes in pressure routing by formulating Collaborative Entrapping Scheme (CES). It is observed that incorporating CES in the pressure based routing protocol effectively detects and prevents the virulent nodes from participating in the routing process, but introduces an overhead. To decrease the overhead due to the CES approach, in this paper, a fraction of data packet (Dfrac) only is used to indicate the successful reception which reduces the end to end delay. Simulation results indicate that the proposed Secure Pressure based Routing protocol shows performance improvement compared to the existing Depth Based and Hydro cast Routing protocols even in the presence of multiple malicious nodes.

Keywords: Collaborative Entrapping Scheme (CES), Reverse directional trails technique (RDTT), Virulent nodes, Hydro cast Routing, Underwater Acoustic sensor network.

1. Introduction

Underwater Acoustic Sensor Networks (UASN) comprise of a large number of spatially distributed underwater sensors, autonomous underwater vehicles (AUVs) and surface buoys that collaboratively monitor the aqueous environment, through its sensing, processing and acoustic communication capabilities. Underwater acoustic sensors are either anchored to the bottom of the aquatic environment or may be dangled at the required specific depths or freely floating in the aqueous medium depending on the type of application. The sensors drift [1] with respect to water currents and vortices while the AUVs are mobile.

Underwater Acoustic Sensor Networks find diverse range of applications in the exploration of valuable minerals, reservoirs, in marine ecosystem and performs 3D ocean sampling environment. UASN perceive seismicity from remote areas and impart warnings to coastal areas thus preventing calamity [2]. Sensors in oceans are useful to discern the hazards in the subsea environment, Thus UASN ensures assistance in navigation and monitors areas for tactical surveillance, targeting, and tracking of human activities in undersea environment and intrusion detection and mine reconnaissance systems. Thus it provides environmental assessment for biological and chemical pollution monitoring [3].

The main factors that affect the underwater acoustic communications are low bandwidth, path loss (attenuation, geometric spreading) and noise (man-made noise due to machinery or ambient noise due to hydrodynamics), scattering, refraction, reverberation, Doppler spread, and high and variable propagation delay, dispersion due to depth of the ocean environment. Multi path propagation which eventually leads to Intersymbol Interference due to the temporal and spatial diversity of the acoustic channel [4] affects the acoustic signal propagation in underwater. The propagation speed [5] of the acoustic signal depends on the temperature, pressure and salinity. The nodes are prone to drifting due to various oceanographic forces [6] influenced by various factors like frictional force, gravitational force, centrifugal force and pressure gradient force (PGF) due to non uniform spatial distribution of pressure.

These distinctive characteristics of Underwater Acoustic Sensor Networks make it highly susceptible to various types of attacks [7]. This paper mainly focuses on one such active attack called black hole attack and its extension which is gray hole attack. In this attack, the virulent node transmits the counterfeit message to the source node that it has the brief route to the Sink. The virulent node captures all the data packets in response to its counterfeit route reply claiming that it has the shortest path to the Sink and then it casts away the captured data packets. Thus the entire communication between the source node and the sink is interrupted.

In this paper, a novel "Secure Robust Pressure based Routing (SecPR) which incorporates the Collaborative Entrapping Scheme (CES) for security purposes, is proposed with the aim of detecting and preventing the virulent nodes causing Black hole and grey hole attacks. The depth of the stochastically chosen node is used to lure the virulent node to send the counterfeit message. By commencing the Reverse Directional Trail Technique (RDTT), the virulent nodes are detected and are placed in the segregated list. In order to prevent the gray hole attacks and mitigate the

*E-mail address: bhairavi@pec.edu

ISSN: 1791-2377 © 2018 Eastern Macedonia and Thrace Institute of Technology. All rights reserved.
doi:10.25103/jestr.115.02

virulent nodes from participating in the routing process, Bidirectional Checkout Phase (BCP) is actuated. However, it is observed that incorporating CES in the pressure based routing protocol introduces an overhead. To decrease the overhead due to the CES approach, in this paper, a fraction of data packet (D_{frac}) only is used to indicate the successful reception which reduces the end to end delay, thereby improving the overall network performance.

The structure of the paper is organized as follows : In Section II, the overview of various routing approaches in Underwater Acoustic Sensor Network is summarized. In Section III, the proposed Secure Robust Pressure based Routing incorporated with Collaborative Entrapping Scheme (CES) is described. In Section IV, the simulation results of the proposed scheme and its comparison with the existing Depth Based Routing and Hydrocast Routing protocol is presented. Finally, the conclusion is made in Section V.

2. Related Works

Several authors have proposed routing protocols for Underwater Acoustic Sensor Networks which are discussed in this section. Xie et al. [8] proposed the Vector Based Forward routing protocol with self-adaption algorithm. The coordinates of the source and the destination nodes are used to compute the routing vector. A routing pipe is formulated between the sender and the destination nodes by utilizing the preordained radius. Intermediate nodes upon the reception of data packets, participates in the routing process if its distance is less than the predestined radius of the routing pipe and then computes its desirableness factor which determines its appropriateness in participating in the forwarding process[9]. However, the main drawback of this routing protocol is that energy consumption of the network is very high.

Shi, Z.J et.al. proposed in [10] the Depth-Based Routing (DBR) protocol. Each sensor node is capable of computing its own depth. The packet forwarding is done avariciously depending on the measured pressure levels. Whenever a node receives the broadcasted data packets, each node compares its own depth (D_a) with the depth of the previous sender (D_s). If the sender is at a shallow depth ($D_a > D_s$), then the current node suppresses its own transmission. Packet forwarding nodes are selected greedily with lower depths. In DBR all sensors require a depth sensor and this requirement inturn increases the overall cost of the routing process.

The Hop-by-Hop Dynamic Addressing Based (H2-DAB) routing protocol [11] is an elementary routing protocol that does not require any 3 dimensional geographic location coordinates of the sensor nodes. The sensor nodes are allocated with an unique routable address comprising of a node ID and a hop ID. The dynamic addressing capabilities makes H2DAB, independent from any static infrastructure based configuration and allows the network to be completely dynamic and self-configurative. Upon the reception of inquiry packet from the source node, the neighbouring nodes replies specifying its routable address. The node with minimum hop ID is chosen as the next hop neighbour node. Before the actual routing process, Due to the inquiry and reply packet transmissions of routable addresses between the nodes, long delay is encountered in the network operation.

Void-aware pressure routing (VAPR) proposed by Noh et al. [12], comprises of enhanced beaconing phase followed by avariciously opportunistic directional data forwarding. Each beacon message is adjoined with the depth of the source node, chronological sequence number, directivity of data transmission, hop number and transmitted to the entire network. Upon the reception of beacon information, each node simultaneously updates its routing table with the adjoined information. The main drawback of VAPR is its requirement of beaconic propagation through the entire network. The proactive maintenance of the path makes this routing protocol suitable for static or slow mobile environment

W. Wang et al., proposed in [13] a method to detect the wormhole attacks. By utilizing the round trip time of the acoustic signal, sensor is capable of computing its distance to other nodes in the 3D network. By exploiting the Multidimensional scaling, each sensor node computes the virtual network configuration. Thus the contradictions due to wormhole attacks can be conceived. Angle and edge length distortions can be deliberately calculated by attibutes between the estimated distance and the reconstructed connections. The network is prone to iterative errors which in turn affects the overall network performance.

L. Buttyan and J.P. Hubaux proposed a unique method [14] for the detection of wormhole attack by determining the actual distance between two nodes through appropriate localization techniques and verifies whether the distance is greater than the acoustic transmission range. If the above criteria is satisfied, then the presence of wormhole in the network is witnessed. After the detection it does not have any authentic mechanism for the prevention of wormhole attacks.

Lee et al. [15] proposed Pressure routing protocol also called as Hydrocast routing protocol effectively routes data packets to the sink utilizing the priority of each sensor node computed with respect to the depth information of the sensor and the Normalized Advancement (NADV). In order to overcome the hidden terminal problems a cluster of next hop forwarding set is greedily computed. Each node periodically checks whether it is in the void region. If it is so, it searches for a shallower node whose depth is lower than its depth and precisely maintains a path to that node. These characteristics of pressure routing makes it highly vulnerable to active attacks. Its drawback is that it does not have any security mechanisms to detect and prevent the virulent nodes in the network.

Mukhtiar Ahmed et al. [16] studied various issues in designing routing protocols in UWASN. The issues in the deployment of sensor nodes in the network, dynamic network topology, data forwarding techniques and route discovery mechanisms were analyzed and their performances were studied by numerical simulations.

3. Proposed Approach

Studies on related works indicate that the existing routing protocols for UWASN lack security mechanism. This paper intends to detect and prevent the virulent nodes causing black hole attacks in Pressure based Routing for UWASN by incorporating the Collaborative Entrapping Scheme (CES). The proposed scheme called as SecPR uses the CES as the security mechanism to detect and prevent virulent nodes. In CES, the source node randomly chooses a node (N_E). The depth of this node (N_E) is used as entrapping depth to lure the virulent nodes to send Route Reply. By utilizing the directional trails of the Route Reply, the virulent nodes causing black hole attacks are detected and prevented from taking part in the routing process.

Collaborative Entrapping Scheme (CES) comprises of 3 phases : a) Embarking Phase b) Revelation Phase of Virulent Nodes and c) Despatching Phase. In the Despatching phase the network is free from any malicious nodes and the final routing process is activated. It should be accentuated that the proposed CES scheme is capable of detecting multiple virulent nodes in the network simultaneously. The flowchart for the Collaborative Entrapping Scheme (CES) is described in Fig.1.

a) Embarking Phase

The main aim of the embarking phase is to instigate the virulent nodes to send its route reply. The source node indiscriminately selects and collaborates with its one hop neighbouring node (N_E) whose depth is used to entice the virulent node. Before actuating the routing process, the source node broadcasts the lure Route Request. If only the node (N_E) had sent the reply, then no malicious node is present in the network. The source node deliberately commences the Despatching Routing Phase. If there is any virulent node in the network, upon the reception of the route request, will send a counterfeit Route reply.

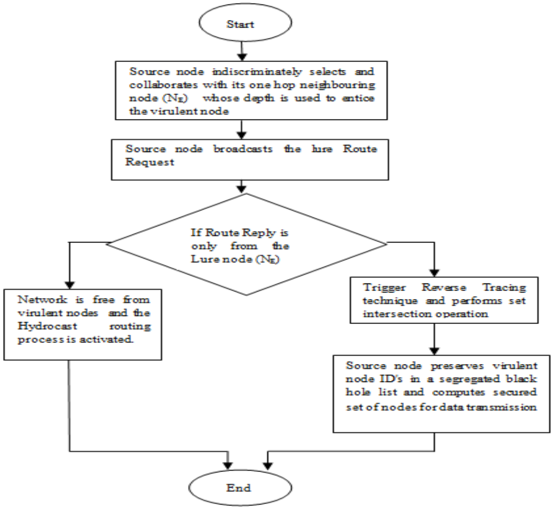
Start
Source node indiscriminately selects and collaborates with its one hop neighbouring node (NE) whose depth is used to entice the virulent node
Source node broadcasts the lure Route Request
If Route Reply is only from the Lure node (NE)
Network is free from virulent nodes and the Hydrocast routing process is activated.
Trigger Reverse Tracing technique and performs set intersection operation
Source node preserves virulent node ID's in a segregated black hole list and computes secured set of nodes for data transmission
End

Fig. 1. Flowchart for Collaborative Entrapping Scheme (CES)

b) Revelation Phase of Virulent Nodes :

Reverse directional trails technique (RDTT) is incorporated to find the virulent nodes from their sham route reply. The prime aim of the Reverse Directional Trail Technique is to infer the suspicious route information of the virulent node. It aids in discovering the transitory un-hazardous region in the route.

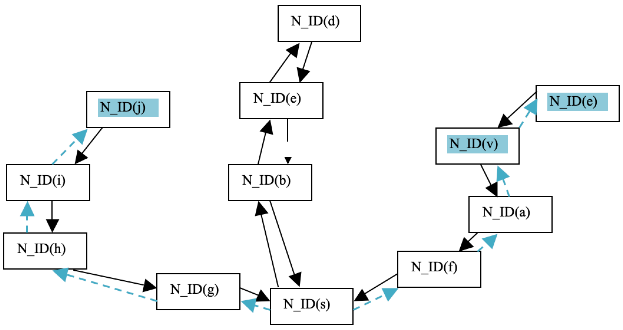

Fig. 2. Reverse Directional Trail Technique

To illustrate The Reverse Directional Trail Technique (RDTT), consider the network depicted in the Fig.2 when multiple virulent nodes exists in the network, the source node in collaboration with the lure node N_D, broadcasts a path request and dissembles to send data packets to node N_D. As a result, of embarking phase, Virulent nodes in the network responses with its counterfeit Route reply embedded with its node id, N_ID(i) computed with respect to the depth of the sensor node D_(i) from the sea surface. The node list is computed as M = {N_{ID}_(s), N_{ID}_(a) N_{ID}_(b), N_{ID}_(c), N_{ID}_(d), N_{ID}_(e), N_{ID}_(f), N_{ID}_(g), N_{ID}_(h), N_{ID}_(i), N_{ID}_(j), N_{ID}_(v)}.Node N_{ID}_(d) is a stochastic random node by node N_{ID}_(s).When node N_{ID}_(a), receives the counterfeit reply from N_{ID}_(v), it will differentiate the set M by the destination node ID N_{ID}_(s), and obtain the list L_(a) = { N_{ID}_(s), N_{ID}_(a), N_{ID}_(f)}. By performing the difference between M lists and L_(a) Lists, L_(a)'= M-L_(a) = {N_{ID}_(v), N_{ID}_(e)}. Node N_{ID}_(a), responses with L_(a)' to the node N_{ID}_(s) with respect to M list. Similarly, node N_{ID}_(f) will carry out the same operation, and generate the list L_(f)= { N_{ID}_(s), N_{ID}_(f)} and L_(f)' = { N_{ID}_(a), N_{ID}_(v), N_{ID}_(e)}. The generated lists are forwarded to the source and the suspicious route information is computed by performing the set intersection operation.

U_1 = L_(a)' ∩ L_(f)' = { N_{ID}_(v), N_{ID}_(e)} is acquired.

The sender node computes the secured set M - U_1 = V_1 = { N_{ID}_(s), N_{ID}_(f), N_{ID}_(a)}.

Likewise, another virulent node N_{ID}_(j), in the network, sends its counterfeit route reply to the node N_{ID}_(i), leading to the subsequent generation of L_(i) = { N_{ID}_(s), N_{ID}_(g), N_{ID}_(h), N_{ID}_(i)} and L_(i)'={ N_{ID}_(j)}. Subsequently, nodes N_{ID}_(h), N_{ID}_(g) iteratively perform the same operation and generate L_(h)' = { N_{ID}_(i), N_{ID}_(j)} and L_(g)' ={ N_{ID}_(i), N_{ID}_(j), N_{ID}_(h)}. The virulent node is identified by, U_2 = L_(i)' ∩ L_(h)' ∩ L_(g)' = { N_{ID}_(j)}. From the generated lists U_1 and U_2, it is understood that CES is capable of detecting multiple number of malevolent nodes causing black-hole attack in the Underwater Acoustic Sensor Network. The sender preserves the virulent node's ID in a segregated list and remaining nodes in the network are forewarned and future communications with the virulent nodes are ceased.

C) Despatching Phase :

After the termination of the Reverse Directional Trail Technique (RDTT), the network is liberated from any virulent nodes and the Pressure based routing process is activated. In the Despatching phase, the entire data transmission happens after the initialization of pressure based routing process which utilizes Normalized Advancement (NADV) for the selection of forwarding cluster of nodes.

Forwarding Cluster Based on Prioritization

As the distance is increased to a farther extent, the effect of attenuation and spreading losses is comparatively more and thus leads to subsequent increase in packet loss. Normalized Advance is defined as the advancement of data packets towards the sink normalized with respect to the corresponding cost [17], NADV= $Pac_{(adv)}$/Cost. Parameter NADV aids in computing the most desirable path to the sink. In other words, NADV can be analyzed with respect to successful advancement of packets to the sink node and their probability of successful delivery as NADV=$P_D^{(i)} X\, A_S^{(i)}$, Where, $P_D^{(i)}$ is the probability of successful delivery of node (i) and $A_S^{(i)}$ is the advancement to the sink node. The Probability of failure is computed using the bit error probability , $P_{failure}$ =$(1-(1-P_{bit-error})$.

When the source node initializes the data transmission, the cluster head nodes upon the reception of packets will analyze their priority. The nodes with the highest priority becomes the next immediate forwarder and initializes its acknowledgement to become successive forwarding node. Let the priority of node x be P_x ,forwards its acknowledgement to the sender node, On sensing the acknowledgement the low priority node say node y with priority (p_y), will restrain its transmission if the following condition ($P_x > P_y$) is satisfied.

However, in the presence of gray hole attacks, a node may perform virulently for a definite period of time and eventually after some time act as a regular trustful node. The condition become worse if the node N_E which is used for the entrapping the virulent nodes in the network is itself a gray hole node.

Thus to overcome the gray hole issues, we incorporate Bidirectional Checkout Phase (BCP) in the dispatching phase.

D) Bidirectional Checkout Phase :

The probability of the forwarding route with at least one virulent node $P(F_R)$ is computed using the following equation,

$$P(F_R) = 1 - (1 - P(V))^h$$

Where, $P(V)$ is the probability that the forwarding route exhibits virulent characteristics and h is the estimated intermediate hops between the Source node and the Destination node.

In the computed trusted node set, after some time when a nodes turns out to become a virulent node, Then these gray hole nodes in the routing process can be detected using the Bidirectional Checkout Phase (BCP). The BCP achieves the above stated goal by using tokens specifying successful reception of data packets. In the trusted set, The intermediate nodes between the source and destination are divided into various triplets say,

{N_{ID}_(b) ➔ N_{ID}_(e) ➔N_{ID}_(c)}

When a node N_{ID}_(b) forwards the data packet from source node to N_{ID}_(e) subsequently N_{ID}_(e) forwards it to N_{ID}_(c) and so on. Due to the instability of nodes certain trusted nodes may also exhibit virulent characteristics after some time. Thus N_{ID}_(b) is unobvious whether N_{ID}_(c) has successfully received data packet. Thus Bidirectional Checkout Phase (BCP) requires a precise token sent by N_{ID}_(c) in the reverse direction to N_{ID}_(b). This token is used to indicate N_{ID}_(b) that N_{ID}_(c) has successfully received the data packets. In each triplet to detect the nodes exhibiting gray hole characteristics, the prime sender preserves a set of node IDs to which the packets are forwarded but not acknowledged. The frame structure of the prime sender of the triplet is shown in Fig.3.

Next hop neighbouring NodeID (N_{ID}_(e))	Second Hop neighbouring NodeID N_{ID}_(c)	$R_{packets}$ Data packets transmitted	R_{fail} BCP Tokens failed	Set of node ID's

Fig. 3. Data Structure maintained by the prime sender of the triplet

Here N_{ID}_(b) preserves this list. At N_{ID}_(b), each node ID will be preserved for a certain period of observation ($T_{attention}$). A node ID will be removed if the token specifying acknowledgement corresponding to this node reaches before the end of the observation period, else at the end of the observation period, the register specified as R_{fail} is incremented and the Node id is placed in the gray hole list. To decrease the overhead due to the CES approach in routing process, a fraction of data packet (D_{frac}) is used to indicate the successful reception. The routing overhead can be varied by subsequent adjustment of D_{frac} .

N_{ID}_(b) carefully notices the activities and the attributes of the link N_{ID}_(e) ➔N_{ID}_(c) for a duration expressed as $T_{attention}$. At the termination of this duration of observation $T_{attention}$, the prime sender computes the ratio of the failed tokens specifying acknowledgement (R_{fail} /$R_{packets}$). The prime sender (N_{ID}_(b)) of the triplet sends out the virulent grayhole report packets. The nodes upon the reception of this grayhole report packets adds the (N_{ID}_(e) ➔ N_{ID}_(c)) links in the segregated list. BCP is carried out at periodic intervals to determine the virulent gray hole nodes and their characteristics in the network.

4. Performance Evauation

The performance of the proposed SecPR protocol is evaluated via simulations in Aquasim (NS 2.30) and the parameters for simulations are listed in Tab.1. Aquasim can efficiently configure and simulate the Real Underwater Acoustic Channel incorporating the Object oriented design of NS-2. The nodes are deployed in region of 1200 x 1200 x 1200 m and the number of sensor nodes are varied from 50 to 150 while the number of virulent nodes is kept constant. Similarly, the network scenarios is studied varying the percentage of virulent nodes as 10 % to 50% through simulations considering the three performance metrics : Packet Delivery Ratio, Throughput and End to End Delay.

In the simulations, the effects of node drifting caused due to wave, currents or tides_ and other oceanographic forces, in the network are validated by utilizing Meandering Current Mobility (MCM) [12]. The elementary forwarding cluster selectivity approach employed in DBR [10] was evaluated. DBR is the first and foremost routing protocol employed in the subsea environment that utilizes the depth factor of each node to route the data packets.DBR routes data in an opportunistic forwarding manner. Opportunistic forwarding nodes are higher than the current forwarder by more than a depth threshold (h) function. DBR is used for comparison along with the pressure based routing protocol also called as Hydrocast Routing protocol [15].

The duration of observation $T_{attention}$ = 0.8 second.

From Fig.4, it can be perceived that when the percentage of malicious nodes is increased, Depth Based Routing [10] and Pressure based Routing (Hydrocast) [15] suffer from dropping attacks. The existing DBR and Hydrocast routing protocols do not have any security mechanisms for detecting/preventing virulent nodes. The proposed SecPR approach shows a higher packet delivery ratio when compared to existing Depth based Routing and Hydro cast Routing Protocols. Considering the worst case network scenario having virulent nodes of about 50%, the proposed SecPR still maintains a Packet Delivery Ratio of about 81%. It can be inferred that SecPR with BCP in the dispatching phase effectively maintains a PDR of about 81% to 95% when the percentage of virulent node is increased from 10% to 50%.

Table 1. Simulation Parameters

Parameters	Value
Simulator	Aquasim (NS2.30)
Simulation Area	1200x1200x1200 m
No. of Nodes	50
Anchored Depth	1100 m
Mobility Model	Meandering Current Mobility(MCM)
Physical layer Model	Underwater Channel
Interface Queue Type	Underwater Phy
Link Layer	DropTail/PriQueue
MAC Protocol	UnderwaterMac/BroadcastMac
Propagation Model	Underwater Propagation
Traffic Model	Underwater Channel
Channel Type	
Speed of Sensor Nodes	(0.4 -0.8) m/s
Simulation Time	100 s
Packet Size	1024 bits
Range of Sensor Node	50-100 m
Malicious Node Ratio	0-50 %
Channel Model	Rayleigh Fading Channel

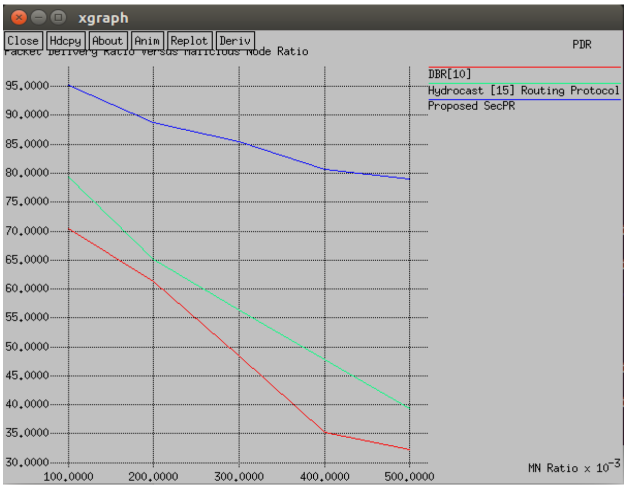

Fig. 4. Packet Delivery Ratio Versus Malicious Node Ratio

In the Fig.5, the Packet Delivery Ratio of the proposed SecPR scheme as a function of percentage of virulent node ratio for different speeds of the sensor nodes (S_n) is analyzed. It is observed that the Packet Delivery Ratio reduces when the mobility increases.

In Fig. 6, we compare the PDR value of the proposed SecPR scheme and the existing Hydrocast routing scheme without any security mechanism for TCP sessions. Comparatively close PDR values for both the proposed and the existing schemes is observed.

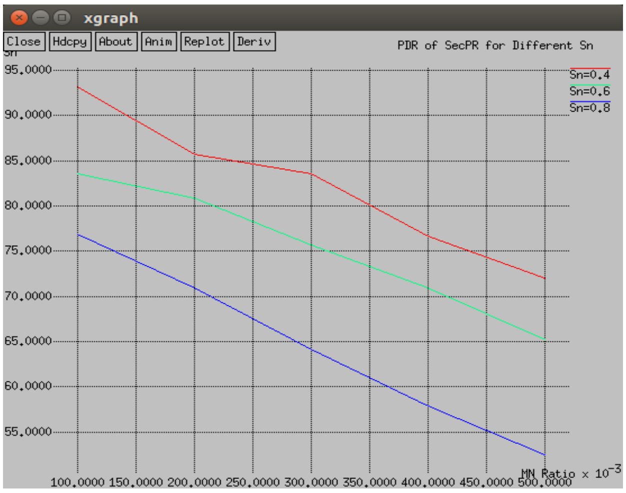

Fig. 5. Packet Delivery Ratio of SecPR for different S_n

This is considered likely or probable to happen as the senders of the TCP sessions slow down or even stop their transmissions when the acknowledgments from the destination are missing. Analyzing the simulation results in Fig.5 and Fig.4, it is perceived that the proposed scheme supports slightly higher Packet Delivery Ratio for TCP traffic than for the UDP traffic. This is caused due to added acknowledgement and route selection in the TCP protocol.

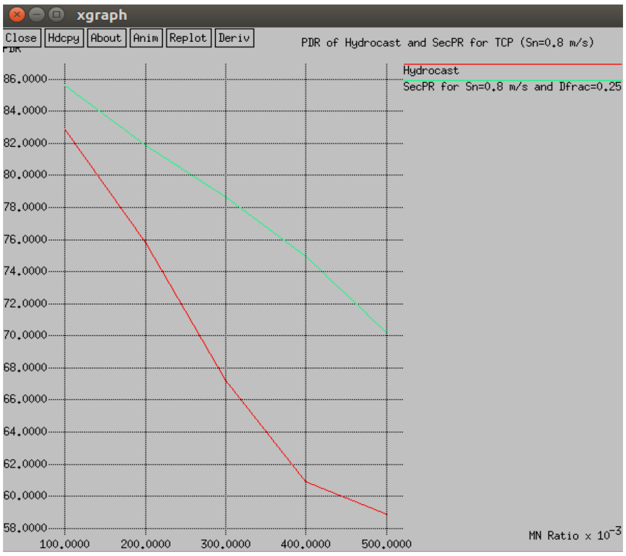

Fig. 6. Packet delivery ratio of SecPR and Hydrocast for TCP (S_n= 0.8 m/s).

The performance of proposed SecPR protocol is compared with existing DBR and Hydrocast in terms of throughput. From the Fig.7 it can be inferred that the existing routing protocols suffer to a greater extent due to the virulent nodes when compared with the proposed SecPR in terms of throughput. It is observed that, when the percentage of virulent nodes is drastically increased to 50%, the proposed SecPR maintains a throughput of about 8000 bits/second by successful detection and prevention of black hole and gray hole nodes from participating in the routing process. It can be observed that, on an average the proposed SecPR during implementation maintains a throughput of 8,000 to 16000 bits/second.

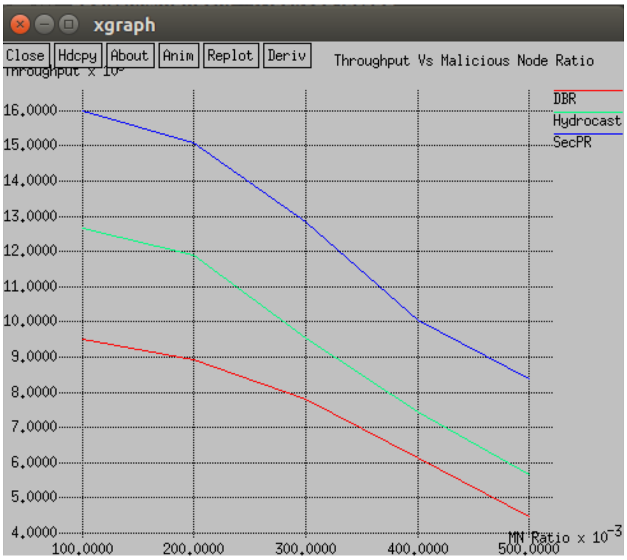

Fig. 7. Throughput Versus Malicious Node Ratio

The performance of the proposed SecPR is compared with existing DBR and Hydrocast in terms of routing overhead for D_{frac}=0.2 and D_{frac}=0.05. From Fig.8, when D_{frac}=0.2, it can be observed that the existing DBR and Hydrocast protocols have low routing overhead compared with SecPR. This is due to the fact that the existing Routing protocols do not have any built-in security mechanism. When the percentage of virulent nodes are increased, the routing overhead of the proposed SecPR is increased due to the multiple route request and acknowledgement packets in the CES approach to discover the trusted path in the network. However, when the Dfrac=0.05, the routing overhead is lower than the existing DBR and Hydrocast routing protocols. Hence the proposed SecPR not only provides security against gray hole attacks but also improves the network performance as it reduces the end to end delay.

The routing overhead of the proposed SecPR for different D_{frac} values is compared in Fig.9. When D_{frac}=1, the routing overhead of the proposed SecPR is very high. When the value of D_{frac} is reduced, the routing overhead of the proposed scheme decreases consequently. Thus, the parameter D_{frac} plays a vital role in adjusting the routing overhead of the system.

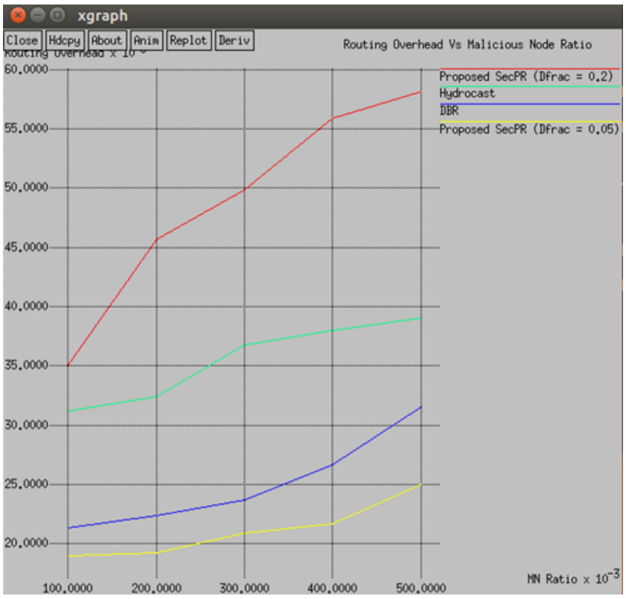

Fig. 8. Routing Overhead Versus Malicious Node Ratio

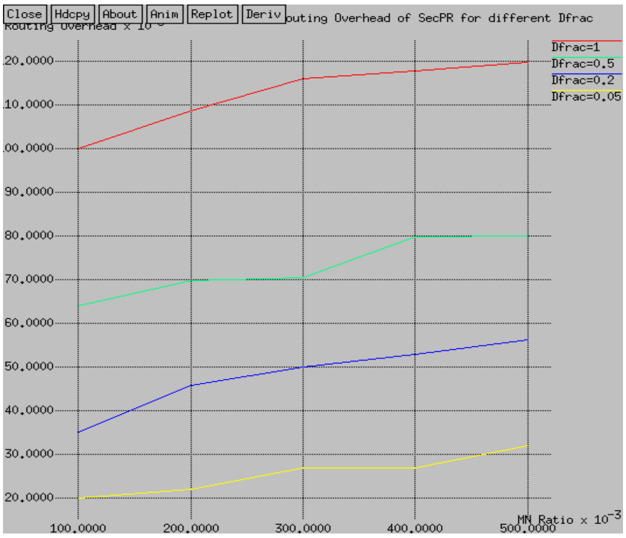

Fig. 9. Routing Overhead of SecPR for different D_{frac}

Finally, the performance of the proposed SecPR approach is compared with existing DBR and Hydro cast protocols in terms of the end-to-end delay. As shown in Fig.10, it can be observed that the proposed scheme has a reduced end-to-end delay when compared with the existing DBR and Hydro cast when the D_{frac}=0.05. Thus, the Proposed SecPR is capable of performing efficiently even in the presence of multiple virulent node.

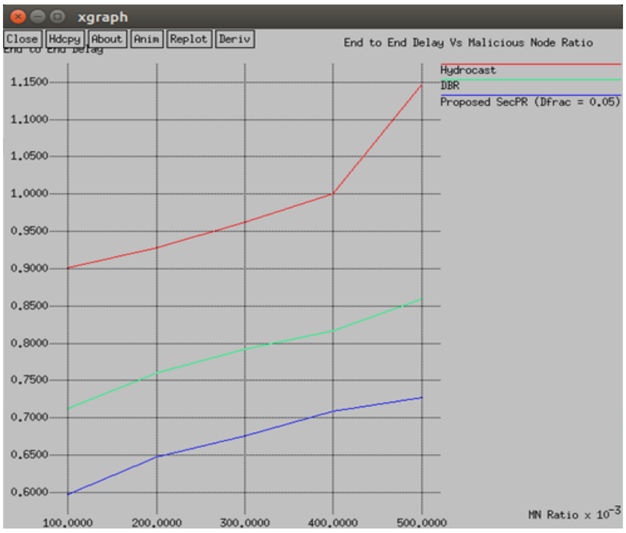

Fig. 10. End to End Delay versus Malicious Node Ratio

From the extensive simulations, it can be inferred that the proposed SecPR has improved performance as well as improved security compared to the existing routing protocols for UWASNs.

5. Conclusion

In this paper, a Secure Pressure routing protocol incorporating Collaborative Entrapping Scheme (CES) with Bidirectional Checkout Phase (BCP) is proposed that effectively detects the virulent nodes in the UWASN. Revelation Phase of Virulent Nodes utilizes Reverse directional trails technique (RDTT) to infer the suspicious path of the virulent node. Simulation results validate that, the proposed SecPR protocol for UWASN shows considerable improvement in network performance during dropping attacks. As a future work, it is aimed to incorporate other encryption schemes to address other types of attacks in UWASN

References

[1]. A.Caruso, F.Paparella, L.F.M.Vieira, M.Erol, and M.Gerla. “The meandering current mobility model and its impact on underwater mobile sensor networks,” *In Proceedings of 27th IEEE Infocommunication,*USA, pp. 771–779, (2008).

[2]. N.N.Soreide, C.E.Woody, and S.M.Holt. "Overview of ocean based buoys and drifters: present applications and future needs," *In Proceedings of the MTS/IEEE Conference and Exhibition OCEANS*, Vol. 4, pp. 2470– 2472,(2001).

[3]. B. Zhang, G.S.Sukhatme, and A.A.Requicha. " Adaptive sampling for marine microorganism monitoring," IEEE/RSJ *International Conference on Intelligent Robots and Systems*(IROS), Japan, DOI:101109/IROS.2004.1389546, (2004).

[4]. Milica Stojanovic, James Preisig. “Underwater Acoustic Communication Channels: Propagation Models and Statistical Characterization”, *IEEE Communications Magazine*, Vol.47, No.1, DOI: 10.1109/MCOM.2009.4752682, (2009) .

[5]. H.Ramezani, R.T.Rajan, and G.Leus. “Cramer–Rao lower bound for underwater range estimation with noisy sound speed profile,” arXiv preprint:1404.7313, (2014).

[6]. A.K. Mandal, S Misra, T Ojha, M. S. Dash, M. K. Obaidat "Oceanic forces and their impact on the performance of mobile underwater acoustic sensor networks," *International Journal Of Communication Systems,* DOI: 10.1002/dac.2882,(2017).

[7]. Guangjie Han, Jinfang Jiang, Ning Sun, and Lei Shu. “Secure Communication for Underwater Acoustic Sensor Networks,” *IEEE Communications Magazine*, Vol.53, No.8, pp.54-60, (2015).

[8]. P. Xie, J.H. Cui, and L. Lao, “VBF: Vector-based forwarding protocol for underwater sensor networks,” *Proceedings of the 5th International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols, Performance of Computer and Communication Networks; Mobile and Wireless Communications Networks*, pp. 1216–1221,(2006).

[9]. Guangjie Han, Jinfang Jiang, Na Bao, Liangtian Wan, and Mohsen Guizani. "Routing Protocols for Underwater Wireless Sensor Networks", *IEEE Communications Magazine*, pp. 0163-6804, (2015).

[10]. Yan.H, Shi. Z., Cui.J.H. "DBR: Depth-Based Routing for Underwater Sensor Networks," In *Proceedings of the7th International IFIP-TC6 Networking Conference on Adhoc and Sensor Networks, Wireless Networks, Next Generation Internet*, Singapore, pp. 72–86, (2008).

[11]. Ayaz.M, Abdullah.A. "Hop-by-Hop Dynamic Addressing Based (H2-DAB) Routing Protocol for Underwater Wireless Sensor Networks," *In Proceedings of the International Conference on Information and Multimedia Technology (ICIMT)*, Jeju Island, pp. 436–441, (2009).

[12]. Y. Noh, U. Lee, P.Wang, B. S. C. Choi, and M. Gerla. “VAPR: Void-aware pressure routing for underwater sensor networks,” *IEEE Transactions on Mobile Computing*, Vol. 12, No. 5, pp. 895–908, (2013).

[13] W. Wang, Bharat Bhargava, Mario Gerla. “Visualization of Wormholes in Underwater Sensor Networks: A Distributed Approach,” *International Journal of Security and Networks*, Vol. 3, No. 1, pp. 10–23, (2008).

[14]. L. Buttyán and J.P. Hubaux. "Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behaviour in the Age of Ubiquitous Computing," Cambridge University Press, (2008).

[15]. Youngtae Noh, Paul Wang, Uichin Lee. " HydroCast: Pressure Routing for Underwater Sensor Networks," *IEEE Transactions On Vehicular Technology*, Vol.65, No.1, pp.333-347, (2016).

[16]. A. Mukhtiar Ahmed, A.Mazleena Salleh , M.Ibrahim Channa " Routing protocols based on protocol operations for underwater wireless sensor network: A survey", Egyptian Informatics Journal, Vol.19, No.1, pp.57-62, (2018).

[17]. S. Lee, B. Bhattacharjee, and S. Banerjee “Efficient geographic routing in multihop wireless networks,” *in Proceedings of MOBIHOC*, pp. 230–241, (2005).