Indonesian Journal of Electrical Engineering and Computer Science
Vol. 30, No. 2, May 2023, pp. 1002~1010
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v30.i2.pp1002-1010

Distributed resource allocation model with presence of multiple jammer for underwater wireless sensor networks

Sheetal Bagali, Ramakrishnan Sundaraguru
Department of Electronics and Communication Engineering, College of Sir MVIT (SMVIT), Bengaluru, India

Article Info

Article history:

Received Feb 24, 2022
Revised Jan 18, 2023
Accepted Jan 26, 2023

Keywords:

Channel access
Cross layer design
Multiple jammer detection
Reactive jammer
Resource allocation
Underwater sensor network

ABSTRACT

Underwater-wireless sensor network (WSN) are prone to the jamming attacks; mainly in case of reactive jamming. Reactive jamming has emerged as one of the critical security threat for underwater-WSN; this occurs due to the reactive jammer capabilities of controlling and regulating jamming duration. Further reactive jammer possesses low detection probability and high vulnerability; moreover the existing model has been designed in consideration with terrestrial-WSN. Hence these models possesses limited capabilities of detecting the jamming and distinguish among uncorrupted and corrupted packets; also it fails to adapt with the dynamic environment. Furthermore co-operative mechanism of jamming model is presented for utilizing the resources in efficient way; however only few existing work has been carried out through the co-operative jamming detection; especially under presence of multiple jammer nodes. For overcoming research issues this paper presents distributed resource allocation (DRA) model adopting cross layer architecture under presence of multiple jammer. DRA algorithm is designed for allocating resource to jammer user in optimal manner. Experiment outcome shows the proposed DRA model achieves much better detection rate considering multi-jammer environment. Thus aid in achieving much better detection accuracy, packet drop, packet transmission and resource utilization performance.

Corresponding Author:

Sheetal Bagali
Department of Electronics and Communication Engineering, College of Sir MVIT (SMVIT)
Bengaluru, India
Email: sheetal.bagali@gmail.com

1. INTRODUCTION

Underwater-wireless sensor network (WSN) plays vital role for many applications that offers ubiquitous computing namely environment monitoring, weather forecasting; in here sensor devices gets placed throughout the environment which offers continuous services and connectivity. This further leads to improvisation in human life; however traditional WSN gets easily compromised through the jamming technology since wireless link are exposed in nature. Moreover jamming induces several attacks such as sybil attack, denial-of-service attack which directly affect the performance of underwater-WSN [1], [2]. Jamming is firmly defined as the specific interference induced in wireless network through the malicious nodes by reducing the signal-to-noise ratio of receiver side through transmission of interfering wireless signals; further it is observed that jamming is different from the interference or regular noise since it causes the degrade in network performance. Further interference is defined as the unintentional noise form which disrupt the network performance. Moreover unintentional interference occurs mainly due to the communication of other device namely microwave and controller or communication among the same network. Similarly intentional interference occurs through the malicious device that are intended to affect the underwater-WSN. Jamming are induced at various level i.e. from hampering communication to alter information in given legitimate communication. Furthermore to understand the attack on underwater-WSN or to avoid the jamming for efficient communication. There are different types of jammer such as reactive jammer, proactive jammer, hybrid smart jammer and function specific jammer; further it is very important to know the jammer types to attain the optimal placement of jammer. Hence many existing methodologies have been considered through the various researcher and various strategy has been designed to address the issue of jamming [3]. Moreover reactive jammer are the type of jamming where jammer remains silent until authentic initialization of the sensor device takes place over the given channel; this is one of the general jamming and used widely; it requires absolute strong mechanism and efficient mechanism [4] to protect and detect respectively. In addition reactive jammer possesses high vulnerabilities along with low detection probability; moreover apart from the novel characteristic underwater-WSN has limited resource and this further causes the huge challenge in designing the detection model. Generally there are two distinctive mechanism to address jamming namely jamming mitigation and jamming detection [5]; however recent existing jamming mitigation method such as direct-sequence spread spectrum (SSS) aka DSSS or frequency-hoping spread spectrum (HSS) does not have the capabilities for sensor devices and detection model for underwater-WSN and hence it fails to secure the message forwarding.

In recent, several mechanism was developed to detect and mitigate the jamming attack for terrestrial-WSN which is also popularly known as TWSN [6]; in [7] author explored different issue to detect the jamming attacks; here detection methods were developed which uses the various metrics such as packet delivery ratio (PDR), received signal strength (RSS), bit error rate (BER). However these mechanism are only designed for general jamming attacks but fails to detect reactive jamming; further [5], [8] developed a model for detecting the model for terrestrial-WSN; further [7] and [9] presented for underwater-WSN. Moreover several network varieties have been developed that offers mitigation solution; similarly [3], [10] used MAC and multiple frequency bands were used for spreading spectrum [11]. Moreover several pre-selected routing paths were proposed in [12]; however capabilities of jammers are restricted in this approach and further it is powerless to detect the authentic traffic due to the camouflage diversities; however they have an added advantage of destructing the mitigation method. Furthermore several mechanism were developed in last decade which utilizes the spectrum in efficient way and also they addressed the spectrum requirements to be utilized for future applications [13]. These model tends to achieve the optimal spectrum utilization, hence these are referred as optimal-resource allocation scheme (RAS) [13], [14]; in here instead of avoiding the jammer it uses different spectrum instances; it depends on the existing spectrum in efficient way for successful mitigation of jamming. Diamant *et al.* [14] developed a particular co-operative authentication communication for achieving optimal resource allocation; in [15] co-operative communication were developed to select the relay aka hop and in [16] cross layer designed were adopted to select the relay node. The main drawback of these models were that they failed to achieve the efficient resource utilization since they avoided the spatial re-use. Diamant *et al.* [17] developed a spatial reuse mechanism considering mitigating near far node effects [18], [19], but ignored proper scheduling as well as delay in transmission, hence there is a huge chance of packet collision. Further, these model are designed considering presence of single jammer scenarios. Thus, this paper present distributed resource allocation model considering presence of multi-jammer environment adopting cross layer architecture. The distributed resource allocation (DRA) model can detect jammer node and allocate resource to jammed user in optimal manner.

The rest of the paper is organized as follows. In section 2 the paper presents distributed resource allocation model for multi-jammer underwater wireless senor network environment. The section 3 discusses about the outcome achieved by DRA over existing jammer detection and resource allocation algorithm. The conclusion of the work is presented in last section 4 with future direction of distributed resource allocation model.

2. DISTRIBUTED RSOURCE ALLOCATION FOR UNDERWATER WIRELESS SENSOR NETWORK

This work present DRA model for UWSN with the presence of multiple jammer. First present the system and reactive jamming model considering presence of multiple jammer. Second present cross layer design between physical (i.e. radio) and data link (i.e., MAC) layer. Lastly presented a distributed strategy for detecting jammer nodes and allocate optimal resource to device that is affected by jamming nodes.

2.1. System and reactive jamming model

Let's consider an underwater wireless sensor network that is composed of set of O authentic sensor device. Further, each sensor device is composed of source-destination pair of devices. Considering this scenario, the underwater wireless sensor network can be seen as a set of concurrent device-to-device communications similar to [20], [21]. This work assumes that the communicating sensor device queues are always flooded/backlogged, then we can describe each transceiver pairs as a session. We describe the transmitting and receiving devices of each session $o \in O$ as $t(o)$ and $e(o)$, respectively. Further, for performing transmission by authentic sensor device there are set of G orthogonal frequency channels. Then, let's consider that there is multiple jammer device k which has limited power constraint and tries to degrade the throughput performance of authentic sensor device by generating interference on the accessible channel. Further, this work considers that the jammer can emit wideband interference simultaneously across all the accessible channel. The jammer power allocation strategy is denoted as follows (1) and (2):

$$q_k = \left(q_k^g\right)_{g\in G}, \tag{1}$$

where q_k^g is the power given on channel g, thus we obtain,

$$X^U q_k \leq q_k^{\uparrow}, \tag{2}$$

where X depicts an $X * |O|$ vector of 'X', and $q_k^{\uparrow}$ is the maximum power of the jammers. Due to the diversity of frequency channels, the jammer must assign its power constraint in a way that aid in attaining good jamming effect. The jammer has capability to measure the noise level and along with can measure interference induced on each channel with respect to its respective location. Without requiring any added knowledge, every jamming nodes can utilize this as a rough measurement for establishing traffic on each channel in UWSNs. Under such assumption, good jamming effect can be modelled by allocating the power cost on the channel is directly proportional with respect to the anticipated traffic on different channel. Let E_k^g depicts the sensed noise and interference level k on channel g. Therefore, the reactive jamming strategy can be described using as (3).

$$q_k^g = \frac{E_k^g}{\sum_{g\in G} E_k^g} * q_k^{\uparrow}, \forall g \in G. \tag{3}$$

2.2. Cross layer design among physical and data link layer model

This work consider a multihop based UWSN communication where sensor device cooperatively transmit there packet to the destination through intermediate nodes with its communication range. Physical layer information is received through hopping. Rather than transmitting its own traffic, a sensor device can behave as a hop device and cooperatively communicate a packet on behalf of another sensor device. Cooperative communication is attained by dividing or distributing the accessible communication time into two stage. Firstly, the source (sender) broadcast the packet (information) to both the hop device and the receiver (destination). Secondly, the hop device forward the obtained packet to the receiver, which then cumulate these packets and perform decoding. In this work, we consider decode-and-forward based cooperative transmission, under which the hop device forward the message only when the packet collected from the source devices can be decoded successfully. To handle with such dynamic behavior of the jammer, we consider a dynamic hop device selection method policy to allow the sensor device form virtual MISO links. At each time slots, a sensor device that decide not to perform sensing any frequency channel will behave as a hop device for other sensor device if there is an optimistic cooperative gain.

The node optimistically access spectrum by maximizing the channel access probability of jammed node and transmit packet. For enabling such modification opportunistic spectrum access with modifiable spectrum access probability parameter is needed at data link layer. Thus, this work employed slotted multichannel carrier-sense multiple access (CSMA) where node chooses one channel at each instance for carrying out transmission operation. In this work considering certain probability the channel are randomly chosen. Further, there will be case where multiple node will chose same channel in that case a random back-off time counter is initialized. In this case the node that first reaches a counter value zero will get contention for transmitting packet. For keeping collision probability less, in this work the contention window (CW) is kept sufficiently large. Let consider r_o^g, $g \in G$ describing the channel sensing probabilities of node o on channel g and then the node might incur certain delay for carrying out communication for being as an intermediate node for neighboring node due to nonzero probability of node o. Thus we have (4).

$$\sum_{g\in G} r_o^g \leq 1. \tag{4}$$

2.3. Channel access probability estimation of legitimate node under presence of multiple jammer nodes

The behavior of authentic sensor device is obtained as follows. When a sensor device is flooded, it choses its channel sensing probability for each channel. The sensor device will serve as a potential hop or cooperator for other authenticated sensor devices if it decide not to sense any channel. This work utilizes channel accessible probability as the policy space of an authenticated sensor device and can be represented as follows (5) and (6):

$$r_o = \left(r_o^g\right)_{g\in\tilde{G}} \tag{5}$$

with,

$$\tilde{G} = G \cup \{0\}, \tag{6}$$

where r_o^g depicts the sensing probability of channel g, and r_o^0 depicts the probability that o doesn't sense any of the channel. Then, it must satisfy following (7)-(9).

$$r_o^g > 0, \forall o \in O, \forall g \in \tilde{G} \tag{7}$$

$$r_o^g \leq 1, \forall o \in O, \forall g \in \tilde{G} \tag{8}$$

$$X^U r_o = 1, \forall o \in O. \tag{9}$$

Further, the sensing probability strategy of all sensor device in O is expressed as (10):

$$r = (r_o)_{o\in O}, \tag{10}$$

and similarly, the sensing probability strategy of all user except for o can be obtained as (11).

$$r_{-o} = (r_n)_{n\in O/o}. \tag{11}$$

Let us assume that, the estimated size of a authenticated sensor device $o \in O$, is expressed as (12):

$$D_o(r, q_k) = \sum_{g\in G} r_o^g \beta_o^g(r, q_k) D_o^g(r, q_k), \tag{12}$$

where $\beta_o^g(r, q_k) D_o^g$ is the probability that sensor device o is able to resourcefully access the channel, r_o^g is the probability that sensor device o senses frequency channel, and $D_o^g(r, q_k)$ is the attainable size on that channel (through either using a cooperative hop device or by using direct transmission), for a given jamming power strategy q_k and sensing probability strategy r.

Let us assume that $o \in O$ sensor device won the channel access game to perform transmission on channel g. Now we express the expected channel load capacity attainable using direct communication i.e., $D_o^g(q, q_k$ in (12) is computed as (13):

$$D_{o,g}^{direct}(q_k) = C \log\left(1 + \mu_{o,g}^{t2e}(q_k)\right), \tag{13}$$

where C is the data rate of each channel, and $\mu_{o,g}^{t2e}(q_k)$ is computed as (14):

$$\mu_{o,g}^{t2e}(q_k) = \frac{q_o I_o \cdot \left(h_o^g\right)^2}{\left(\varphi_{e(o)}^g\right)^2 + q_k I_{ke(o)} \cdot \left(i_{ke(o)}\right)^2} \tag{14}$$

where q_o is the transmission power of senor device o, I_o^g and I_o are the fading and path loss, respectively, $\left(\varphi_{e(o)}^g\right)^2$is the power of noise at the receiver side of sensor device o depicted as $e(o)$ on channel g. The estimated channel load capacity attainable using direct link can be calculated by meaning all the conceivable channel fading component of all the links among $t(o)$ and $e(o)$, and the jammer device and $e(o)$. Similarly, the cooperative hop transmission, i.e., D_o^g in (12) can be computed. Let us assume that each source device $n \in O/o$ functions as a possible hop device with probability r_n^0. Thus, with respect to certain probability, sensor device o will obtain cooperative gain by one of the potential cooperative sensor devices. In such case, a sensor device o selects $t(n)$ as the hop device, then, the resultant cooperative capacity can be expressed as (15);

$$D_{o,g}^{coperative}(q_k) = \frac{C}{2} log\left(1 + \min\left(\mu_{on,g}^{t2s}, \mu_{o,g}^{t2e} + \mu_{no,g}^{s2e}\right)\right) \tag{15}$$

where $\mu_{on,g}^{t2s} = \mu_{on,g}^{t2s}(q_k)$ and $\mu_{no,g}^{s2e} = \mu_{no,g}^{s2e}(q_k)$ depicts the signal to noise ratio of the link among transmitter to hop device and hop device to receiver, respectively. An important thing to be noted here is, from (14) and (15) the cooperative capacity can be lower or higher than the direct capacity. This is due to ½ coefficient consideration in (15). Thus, the overall estimated capacity attainable by sensor device o over channel g can be computed as (16).

$$D_o^g(r, q_k) = \left(\sum_{n\in O/o} D_{o,g}^{coperative}(q_k) + \sum_{n\in O/o} D_{o,g}^{direct}(q_k)\right) \tag{16}$$

From (16) it can be seen, the above equation can be satisfied only when the probability that more than one cooperative sensor device joins in cooperative transmission is very low. Otherwise, the capacity function will be computed as a summation of the estimated cooperative capacities offered by different cooperative hop device. Further, this work aims to utilize resource efficiently without affecting other contending sensor device. Thus, the objective (i.e., utility) parameter of each sensor device can be expressed as (17),

$$V_o(r, q_k) = \log\left(D_o(r, q_k)\right), \tag{17}$$

and the proposed objective parameter to maximize the resource utilization of sensor device without affecting other legitimate sensor device can be expressed as (18).

$$\begin{aligned} &Given\colon q_k \\ &\underset{r\in(0,1)^{|O|}}{\text{Maximize}}\, V_o(r, q_k) = \sum_{o\in O} V_o(r, q_k) \\ &Subject\ to\colon (7), (8), (9) \end{aligned} \tag{18}$$

This work present a distributed strategy to meet proposed resource utilization objectives of (18). This work adopt an iterative fine-grained (best response) model using cost parameter. At every iteration, each session o tries to maximize its objective parameter minus a cost factor that acts as a penalty incurred/levied to each contending session for being too selfish in selecting its own policies and thus affecting other contending sessions. Since this work assumes that for each authenticated sensor device for which the policy of the jammer, that is, q_k is a given parameter, for easiness, it is not considered in from the objective strategy. Let r^w depicts the sensing probability at certain iteration w. The ideal strategy for certain instance $o \in O$ is depicted as $\gamma_o(r_o, r_{-o}^w)$ can be obtained using (19) and (20):

$$\gamma_o(r_o, r_{-o}^w) = (r_o)^U \left(\gamma_o^g(r_o^g, r_{-o}^w)\right)_{g\in\tilde{G}} - \frac{\omega_o}{2}\|r_o - r_o^w\|^2, \tag{19}$$

where,

$$\gamma_o^g(r_o^g, r_{-o}^w) = \sum_{n\in O/o} \frac{\delta V_n(r^w)}{\delta r_o^g} \tag{20}$$

depicts the negligible reduction of cumulated objective parameter of other time instance because of differences of time instance o's sensing probability with respect to channel g. In this work, the $-\frac{\omega_o}{2}\|r_o - r_o^w\|^2$ is a system controlling parameter with the constant ω_o. The value of which must be carefully selected for assuring to prevent each time instance o from being too conservative in optimizing respective sensing probabilities logs [22] and also at same time assuring good concavity of the respective penalized objective parameter function. Then, for respective sensing probabilities logs of all other nodes r_{-o} and $D_o(r)$ is linear function of r_o considering when r_{-o} and $D_o(r) > V_o(r_o, r_{-o})$ in (17) is concave with respect to r_o. As a result, only the second derivative $\nabla_{r_o}^2 V_o(r_o, r_{-o})$ must be proved to be bounded for $\forall r_{-o} \in \tau_{-o} = (\tau_n)_{n\in O/o}$ with (21).

$$\tau_n = \{r_n | bound\colon (5), (6), (7)\}. \tag{21}$$

The second derivative of $V_o(r_o, r_{-o})$ for respective $r_o$can be mathematically stated as (22):

$$\nabla_{r_o}^2 V_o(r_o, r_{-o}) = \frac{1}{D_o(r_o, r_{-o})}\nabla_{r_o}^2 D_o(r_o, r_{-o}) - \frac{1}{D_o^2(r_o, r_{-o})}\nabla_{r_o} D_o(r_o, r_{-o}). \tag{22}$$

As this work consider the $r_o^g > 0$ for $\forall o \in O,\ g \in G,\ \frac{1}{D_o(r_o, r_{-o})}$, and $\frac{1}{D_o^2(r_o, r_{-o})}$ to be bounded thus both $\nabla_{r_o} D_o(r_o, r_{-o})$ and $\nabla_{r_o}^2 V_o(r_o, r_{-o})$ are bounded for closed τ_n. The (21) and (22) assures good concavity. Thus, here we set $\omega_o = 0$. In our work the penalized objective parameter function is defined using as (23):

$$\tilde{V}_o(r_o, r_{-o}) = V_o(r_o, r_{-o}) + \gamma_o(r_o, r_{-o}^w, 0), \quad (23)$$

with $\gamma_o(r_o, r_{-o}^w, 0)$ described in (20).

Considering the problem in satisfying (18) the convergence can be satisfied using Algorithm 1 assuming that $\{Q^w\}$ is selected so that as (24).

$$Q^w \in [0,1], Q^w \rightarrow 0, \text{and } \sum_w Q^w = +\infty \quad (24)$$

Then, every bounding point of $\{Q^w\}$ is an optimal strategy of (18) or the Algorithm 1 will converge to a finite set of iteration to an optimal strategy of (18). Further, each strategy obtained using algorithm 1 can satisfy (24) as shown in (25):

$$Q^w = \frac{Q^{w-1} + \sigma(w)}{1 + \rho(w)}, w = 1, \dots, \quad (25)$$

where $\sigma(w) = \sigma$ and $\rho(w) = w\rho$ with $\sigma, \rho \in (0,1)$ and $\sigma \leq \rho$. The proposed distributed resource utilization model under presence of multiple jamming nodes attain superior performance than state-of-art model which is experimentally proved in next section.

Algorithm 1. Optimal resource utilization algorithm

```
Step 1. Start.
Step 2. Input data $\{Q^w\} > 0$, set $w = 0$.
Step 3. If $r^w$guarantees an appropriate termination condition
Step 4.    Stop.
Step 5. $\forall o \in O$, evaluate
Step 6.    $\hat{r}_o(r^w) = \arg\max_{r_o \in \tau_o} \tilde{V}_o(r_o, r_{-o})$
Step 7. Set $r_o^{w+1} = r_o^w + \rho^w(\hat{r}_o(r^w) - r_o^w)$.
Step 8. $w \leftarrow w + 1$ and go back to step 2.
Step 9. Stop.
```

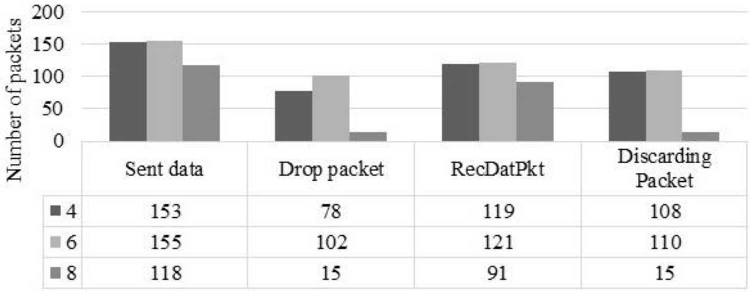
3. RESULTS AND DISCUSSION

This section discusses about the experimental setup and simulation parameter, performance metric used for analyzing outcome achieved by distributed resource allocation model over existing resource allocation model [18] under presence of multiple jamming sensor devices. MAcoSim simulator is used for carrying out performance evaluation [23]-[25]. MAcoSim is implemented in MATLAB on top of NS2 simulation platform and offers very good graphical user interface. The outcome is written on trace file similar to NAM trace file which are later used for graphically representing the outcome. The experiment is carried on similar terms and setup used in [17]. Experiment is conducted by varying sensor mote size of 50, 75, and 100. These motes are placed randomly across UWSN with size of 16m*16m. Further, the jammer mote size are varied from 4, 6, and 8 and placed within 16m*16m area. Each jammer will transmit 8 bits of packet for a give slot and each motes will generate traffic in UWSN by transmitting 3 bits of packets. Total 100 iteration is considered for obtaining simulated outcomes and performance achieved is estimated using successful packet transmission, packet drop, packet error rate and detection rate metrics.

Figure 1 show packet transmission performance achieved by proposed by proposed DRA model with presence of multiple jammer. Here jammer mote size is varied from 4, 6, and 8 keeping UWSN mote size to 100 and experiment is conducted. From experiment is seen when jammer mote size is 4, 6, and 8 the number of sent packet is 153, 155, and 118, respectively. Then, when jammer mote size is 4, 6, and 8 the number of dropped packet is 78, 102, and 15, respectively. Then, when jammer mote size is 4, 6, and 8 the number of received packet is 119, 121, and 91, respectively. Similarly, when jammer mote size is 4, 6, and 8 the number of discarded packet is 108, 110, and 15, respectively. Further, the packet error rate (PER) is computed by varying jammer mote size. When jammer mote size is 4, 6, and 8 the PER achieved by DRA is 0.03252, 0.0163, and 0.0421, considering signal-to-noise-ratio of 4 dB, respectively. From result it can be seen as jammer mote size increases packet being dropped is increasing. However, when jammer mote size 8 very less number of packet is being transmitted; thus very less number of packet being dropped. Very limited work is carried out by existing methodologies for evaluating performance considering presence of multiple jammer. This, work is first of kind to evaluate such kind evaluation considering presence of multiple jammer in UWSN environment. Further, this work evaluate the resource utilization performance of DRA by varying jammer device size.

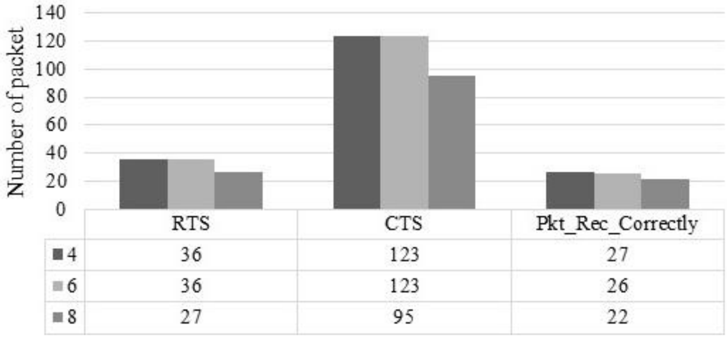
Figure 2 show the resource utilization performance achieved by DRA considering varied jammer mote size. From result it can be seen when jammer mote size is 4, 6, and 8 the total clear to send (CTS) packet sent is 123, 123, and 95. Then when jammer mote size is 4, 6, and 8 the total request to send (RTS) packet sent is 36, 36, and 27. Similarly when jammer mote size is 4, 6, and 8 the total packet received correctly is 27, 26, and 22. From result it can be seen on an average considering varied jammer mote size 33 RTS packet is sent in a UWSN network out of which 25 packets have been successfully received at the receiver side. From this we can interpretive that there is 24.245% duplicate packet generated by jammer is being circulated in UWSN environment by using UWSN resource (i.e., slots). Thus, this work further evaluate performance of DRA by varying slot size.

Figure 3 shows the packet transmission performance achieved by proposed DRA by varying slots size. Here slots size is varied from 3μs, 5 μs, and 10 μs. When slots size is 3 μs, 5 μs, and 10 μs the number of packet sent in UWSN is 146, 164, and 168, respectively. Similarly, when slot size 3 μs, 5 μs, and 10 μs the number of packet is dropped in UWSN is 88, 94, and 90, respectively. Further, it is important to evaluate performance varying sensor mote size keeping jammer mote size constant with 8. Figure 4 shows packet transmission performance considering varied UWSN mote size. The number of packet transmitted is equal to 160, 187, and 219 when mote size is 50, 75, and 100, respectively. Similarly, when mote size is 50, 75, and 100 the number packet dropped is equal to 79, 97, and 119, respectively. From Figures 3 and 4 it can be seen as node size is increased high number of packet being circulated and at the same time packet drop in network also increases.



	Sent data	Drop packet	RecDatPkt	Discarding Packet
■ 4	153	78	119	108
■ 6	155	102	121	110
■ 8	118	15	91	15

Figure 1. Packet transmission performance considering varied number of jammer device



	RTS	CTS	Pkt_Rec_Correctly
■ 4	36	123	27
■ 6	36	123	26
■ 8	27	95	22

Figure 2. Resource utilization performance considering varied number of jammer device

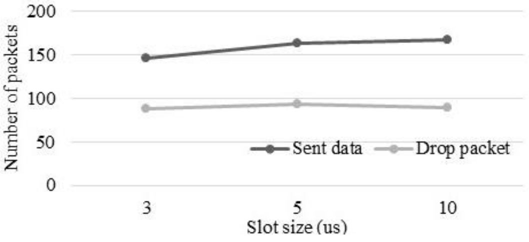


Figure 3. Packet transmission performance for varied slot size

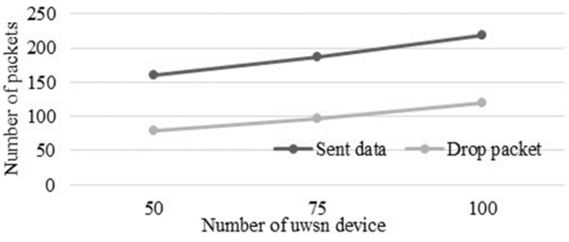


Figure 4. Packet transmission performance for varied uwsn devices

To show the DRA model achieves much superior outcome that existing methodologies [17]; a comparative analysis is shown in Table 1. Total five parameter such as packet drop rate, packet error rate, packet sending ratio, detection accuracy for detecting jamming effect of jammer node, and resource/slots utilization. Existing methodologies [17] have evaluated performance only for detection accuracy, resource utilization, and drop rate. The adoption of spatial spectrum utilization aided in utilizing resource more efficiently. However, drop rate is still extremely high and with presence of external jammer it is expected to even worse. This is because of poor scheduling strategy adopted by their methodology. On the other, the DRA employs distributed scheduling mechanism adopting cross layer design aiding in detecting jammer node efficiently and achieving higher resource utilization. The cross layer design aid in optimizing channel access probability and cooperative communication of non-jammer in distributed manner. The significant resource utilization performance is because of higher number of transmission and less number of packet being dropped. This is because channel load capacity of UWSN device are evaluated by maximizing resource allocation in distributed without causing much interference to neighbouring motes. Further, the jammer node are effectively identified with better detection accuracy aiding packet transmission and resource utilization performance with minimal packet error rate.

Table 1. Performance comparison of DRA with respect to existing resource allocation model [17] under UWSN environment

Parameter	[17]	Proposed DRA
Drop rate	33.33%-57.15%	5.34% to 11.51%.
Packet error rate	-	0.0163 to 0.0421.
Packet Sending ratio	-	96.9703%.
Detection accuracy	-	85.153%.
Resource utilization	90.0%	98.83%.

4. CONCLUSION

This work presented distributed resource allocation model for jammed user under presence of multiple jammer sensor device. The DRA model can detect jammer node more efficiently and allocate resource to jammed node in more optimal fashion meeting resource maximizing constraint. The adoption of distributed strategy aid in detecting jammer more efficiently. Further, cooperative cross layer design aid in utilizing resource more efficiently. Then, keeping contention window larger aid in reducing packet drop in network. The DRA model can distinguish between the corrupted and uncorrupted parts of a packet. As a result, they are efficient in identifying jamming nodes. From result achieved it can be seen the DRA model achieves packet drop rate of 5.34%-11.51% where existing methodologies achieves a drop rate of 33.33%-57.15%. Further, existing methodologies achieves resource utilization 90% where the DRA achieves a resource utilization performance of 98.83%. Further, the proposed DRA achieves packet error rate, packet sending ratio, and detection accuracy of 0.0163 to 0.0421, 96.9703%, and 85.153%, respectively under multi jammer environment. From result achieved it can be sated the DRA is very efficient when adopted under highly dynamic jamming environment with presence of multiple jammer. Future work would consider improving DRA resource utilization performance and evaluate model energy efficiency under more complicated jamming effects.

REFERENCES

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

[2] A. Wood, J. Stankovic, and G. Zhou, “DEEJAM: Defeating energy efficient jamming in IEEE 802.15.4- based wireless networks,” *in: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2007, pp 60–69, doi: 10.1109/SAHCN.2007.4292818.

[3] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: Attack and defense strategies,” *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006, doi: 10.1109/MNET.2006.1637931.

[4] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks—how realistic is the threat?," *in: WiSec '11: Proceedings of the fourth ACM conference on Wireless network security*, pp. 47–52, 2011, doi: 10.1145/1998412.1998422.

[5] M. Strasser, B. Danev, and S. Capkun, “Detection of reactive jamming in sensor networks,” *ACM Transactions on Sensor Networks*, vol. 7, no. 2, pp. 1–29, 2010, doi: 10.1145/1824766.1824772.

[6] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: the case of jammers,” *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 245–257, 2011, doi: 10.1109/SURV.2011.041110.00022.

[7] S. Misra, S. Dash, M. Khatua, A. V. Vasilakos, and M. S. Obaidat, “Jamming in underwater sensor networks: detection and mitigation,” *IET Communications*, vol. 6, no. 14, pp. 2178–2188, 2012, doi: 10.1049/iet-com.2011.0641.

[8] D. Giustiniano, V. Lendersy, J. B. Schmittz, M. Spuhler, and M. Wilhelmz, “Detection of reactive jamming in DSSS-based wireless networks,” *in: WiSec '13: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, , 2013, pp. 43–48, doi: 10.1145/2462096.2462104.

[9] M. Khatua and S. Misra, “Exploiting partial-packet information for reactive jamming detection: studies in UWSN environment,” *in: Proc. of the 14th International Conference on Distributed Computing and Networking,* 2013, pp. 118–132, doi: 10.1007/978-3-642-35668-1_9.

[10] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, “A trigger identification service for defending reactive jammers in WSN,” in *IEEE Transactions on Mobile Computing,* vol. 11, no. 5, pp. 793-806, May 2012, doi: 10.1109/TMC.2011.86.

[11] S. Jiang, “State-of-the-art medium access control (MAC) protocols for underwater acoustic networks: a survey based on a MAC reference model,” *in IEEE Communications Surveys and Tutorials,* vol. 20, no. 1, pp. 96-131, 2018, doi: 10.1109/COMST.2017.2768802.

[12] P. Tague, S. Nabar, J. A. Ritcey, and R. Poovendran, “Jamming aware traffic allocation for multiple-path routing using portfolio selection,” *IEEE/ACM Transactions on Networking*, 2010, doi: 10.1109/TNET.2010.2057515.

[13] P. Bhavathankar, S. Sarkar, and S. Misra, “Optimal decision rule-based ex-ante frequency hopping for jamming avoidance in wireless sensor networks,” *Computer Networks,* vol. 128, pp. 172-185, 2017, doi: 10.1016/j.comnet.2017.03.009.

[14] R. Diamant, P. Casari, and S. Tomasin, “Cooperative authentication in underwater acoustic sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 954-968, Feb. 2019, doi: 10.1109/TWC.2018.2886896.

[15] M. A. M. Sadr, M. Ahmadian-Attari, R. Amiri, and V. V. Sabegh, “Worst-case jamming attack and optimum defense strategy in cooperative relay networks,” in *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 7-12, 2019, doi: 10.1109/LCSYS.2018.2850658.

[16] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, “Toward the development of secure underwater acoustic networks,” in *IEEE Journal of Oceanic Engineering,* vol. 42, no. 4, pp. 1075-1087, Oct. 2017, doi: 10.1109/JOE.2017.2716599.

[17] R. Diamant, R. Francescon, and M. Zorzi, “Topology-efficient discovery: a topology discovery algorithm for underwater acoustic networks,” in *IEEE Journal of Oceanic Engineering*, vol. 43, no. 4, pp. 1200-1214, Oct. 2018, doi: 10.1109/JOE.2017.2716238.

[18] W. Aman, M. M. U. Rahman, J. Qadir, H. Pervaiz, and Q. Ni, “ Impersonation detection in line-of-sight underwater acoustic sensor networks,” *IEEE Access,* vol. 6, pp. 44459-44472, 2018, doi: 10.1109/ACCESS.2018.2863945.

[19] R. Diamant, P. Casari, F. Campagnaro, and M. Zorzi, “Leveraging the near–far effect for improved spatial-reuse scheduling in underwater acoustic networks,” in *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1480-1493, Mar. 2017, doi: 10.1109/TWC.2016.2646682.

[20] S. Bagali and R. Sundaraguru, “Maximize resource utilization based channel access model with presence of reactive jammer for underwater wireless sensor network,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 3, pp. 3284-3294, 2019, doi: 10.11591/ijece.v10i3.pp3284-3294.

[21] S. Bagali and R. Sundaraguru, “Efficient channel access model for detecting reactive jamming for underwater wireless sensor network,” *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET),* 2019, pp. 196-200, doi: 10.1109/WiSPNET45539.2019.9032861.

[22] H. U. Yildiz, V. C. Gungor, and B. Tavli, “Packet size optimization for lifetime maximization in underwater acoustic sensor networks,” in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 719-729, Feb. 2019 doi: 10.1109/TII.2018.2841830.

[23] A. P. Das and S. M. Thampi, “Simulation tools for underwater sensor networks: a survey,” *Network Protocols and Algorithms,* vol. 8, no. 4, 2016, doi:10.5296/npa.v8i4.10471.

[24] S. Kang, M. Aldwairi, and K.-I. Kim, “A survey on network simulators in three-dimensional wireless ad hoc and sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 10, 2016, doi: 12. 10.1177/1550147716664740.

[25] S. Misra “Macosim: MATLAB-based acoustic underwater simulator,” cse.iitkgp.ac.in, 2015, https://cse.iitkgp.ac.in/~smisra/swan/tre/macosim.html, (accessed on Dec. 15, 2016).

BIOGRAPHIES OF AUTHORS

Sheetal Bagali is Assistant Professor at Sir M. Visvesvaraya Institute of Technology, Bangalore. She received B.E. degree in Electronics and Communication Engineering and M. Tech degree in VLSI and Embedded System from Visvesvaraya Technological University. She is her persuing Ph.D. degree in Underwater Sensor Networks from Visvesvaraya Technological University. Her research areas are underwater communication, VLSI and sensor networks. She has authored more than 10 publications. She can be contacted at email: sheetalbagali_ece@sirmvit.edu.

Dr. Ramakrishnan Sundaraguru is Professor at Sir M. Visvesvaraya Institute of Technology, Bangalore. He has Ph.D in Wireless Communication from Anna University. He has supervised and co-supervised more than 20 masters and 5 Ph.D. students. He has authored or coauthored more than 53 publications. His research interests include wireless sensor network and wireless communication. He has two patents granted in his name. He can be contacted at email: sugursg@gmail.com.