International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 3, June 2020, pp. 3284~3394
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i3.pp3284-3394

Maximize resource utilization based channel access model with presence of reactive jammer for underwater wireless sensor network

Sheetal Bagali, R. Sundaraguru
Department of Electronics and Communication Engineering, Sir M Visvesvaraya Institute of Technology, India

Article Info

Article history:

Received Jun 4, 2019
Revised Dec 11, 2019
Accepted Jan 8, 2020

Keywords:

Cooperative communication
Cross layer design
Jamming detection
Medium access control
Reactive jamming
Spatial reuse
UWSN

ABSTRACT

Underwater sensor networks (UWSNs) are vulnerable to jamming attacks. Especially, reactive jamming which emerged as a greatest security threat to UWSNs. Reactive jammer are difficult to be removed, defended and identified. Since reactive jammer can control and regulate (i.e., the duration of the jam signal) the probability of jamming for maintaining high vulnerability with low detection probability. The existing model are generally designed considering terrestrial wireless sensor networks (TWSNs). Further, these models are limited in their ability to detect jamming correctly, distinguish between the corrupted and uncorrupted parts of a packet, and be adaptive with the dynamic environment. Cooperative jamming model has presented in recent times to utilize resource efficiently. However, very limited work is carried out using cooperative jamming detection. For overcoming research challenges, this work present Maximize Resource Utilization based Channel Access (MRUCA). The MRUCA uses cross layer design for mitigating reactive jammer (i.e., MRUCA jointly optimizes the cooperative hopping probabilities and channel accessibility probabilities of authenticated sensor device). Along with channel, load capacity of authenticated sensor device is estimated to utilize (maximize) resource efficiently. Experiment outcome shows the proposed MRUCA model attain superior performance than state-of-art model in terms of packet transmission, BER and Detection rate.

Corresponding Author:

Sheetal Bagali,
Department of Electronics and Communication Engineering,
Sir M Visvesvaraya Institute of Technology,
Bengaluru, Karnataka 562157, India.
Email: sheetal.bagali@gmail.com

1. INTRODUCTION

Underwater wireless sensor network play a major role across various application services in offering ubiquitous assess such as weather forecasting, marine safety, environment etc. where sensor devices are placed across environment to offer continuous connectivity and services. Thus, aid in improving quality of humans life. However, traditional wireless network can easily compromised by jamming technology. This is due to exposed nature of wireless links. Jamming can induce attack [1] such as Denial-of-Service (DoS) attack, Sybil attack etc. affecting performance of UWSN [2, 3]. Jamming in UWSN can be defined as the interference induced in existing wireless network communication by malicious sensor nodes by decreasing the signal-to-noise ratio (SINR) of the authenticated sensor device (receiver side) by transmitting interfering wireless signals. Jamming is different from regular noise or interference because it is a resultant of deliberate use of wireless signal to degrade network performance whereas as interference is an unintentional forms of noise disrupting performance of UWSN. Unintentional interference caused in network is due to

wireless communication of other device (such as remote controller and microwave) or communication among sensor device within the same network. Whereas, intentional interference is generally carried out by malicious sensor device who intended to affect the communication of UWSN. Jamming can be induced at different level, from delaying or hampering communication to altering packet/information in authenticated/legitimate communication. To understand how jammer attack UWSN and to avoid jamming to attain efficient communication it is important know different types of jammer [4] such as function specific jammer, hybrid-smart jammer, proactive jammer, reactive jammer, and optimal placement of jammer for attaining best jamming effects. Recently, effort has been putted by various researcher and presented defense strategy to address the jamming issues [5]. However, reactive jammer based attack, where jammer device stay quiet until any authentic sensor device initialize (sense) transmission (even if single bit transmission is initialized) over the channel, emerged recently and requires for a stronger defense mechanism and efficient detection scheme [6]. A reactive jammer for maintaining high vulnerability with low detection probability controls the duration of jam signal and the probability of jamming. Further, the unique characteristics and the limited resources of UWSNs [2] make the designing of jamming attack detection model more challenging in these network environments. In general, there exist two method to address jamming attacks on alarm forwarding such as jamming detection and jamming mitigation [7]. However, current spread-spectrum-based jamming mitigation methods such as (direct sequence spread spectrum) DSSS or (frequency hopping spread spectrum (FHSS) FHSS are beyond the capabilities of current sensor device and existing jamming detection model for UWSNs is not efficient to protect the considered reactive message forwarding.

Recently, number of approaches has been presented for detecting and mitigating jamming attack for terrestrial WSNs (TWSNs) [8]. Further, [9] explored various problems in detecting jamming attack in wireless networks, and presented detection methods using different metrics such as bit error rate (BER), received signal strength (RSS), and packet delivery ratio (PDR). However, these methods are designed for detecting general jamming attack, but not specially designed to detect reactive jamming. In [7, 10] presented a model to detect reactive jamming for TWSNs and [9, 11] for UWSNs. Further, various network diversities are explored to offer mitigation solutions [12]. Spreading spectrum [5, 13] making use of multiple frequency bands and medium access control (MAC) channels, Multi-path routing benefiting from multiple pre-selected routing paths [12] are two good examples of them. However, in this approach, the ability of jammers are considered to be restricted and powerless to catch the authenticated traffic from the camouflage of these diversities. However, due to the silent nature or behavior of reactive jammers, they have more powers to destruct these mitigation methods. In recent times, number of approaches has been presented to a utilize spectrum efficiently and address spectrum requirement for provisioning future application [14]. These model aims to attain optimal use of available resource (spectrum). Thus, these model are referred as optimal resource allocation schemes [14, 15]. In optimal resource allocation schemes, the sensor device, rather than avoiding a jammer by using different instance of spectrum, depends on exploring the existing spectrum in most resourceful way to mitigate jamming. Further, [15] presented a cooperative authentication communication to attain optimal resource allocation. Similarly, [16] presented cooperative communication scheme for relay/hop selection and [17] adopted cross layer design for relay node selection. However, these model are not efficient in utilizing spectrum efficiently as they do not consider spatial reuse. In [18] presented topology-efficient discovery algorithm consider spatial reuse for utilizing spectrum efficiently. Though, [18] introduced spatial reuse, without proper scheduling and delays in transmissions, many packets still collide.

For overcoming research challenges, this work presents maximize resource utilization based channel access (MRUCA) model for UWSN using cross layer design. The MRUCA jointly optimizes the cooperative hopping probabilities and channel accessibility probabilities of authenticated sensor device. This work considers that the sensor device cooperate at two stages. Firstly, at the MAC layer, a cooperative channel access model is presented where the channel accessibility probabilities of different sensor devices are optimally controlled so that sensor devices degraded rigorously by jammer have higher portion of transmission time. In this manner, the sensor device with ideal links share capacity with those with jammed links. Secondly, this work extend cooperation among physical and MAC layer. That is, this work use cooperative hop based transmission with certain probability for increasing the link capacity of sensor device in UWSNs. Lastly, channel load capacity is estimated to maximize resource utilization. The rest of the paper is organized as follows. In section II literature survey is discussed. In section III the proposed maximize resource utilization based channel access model for underwater wireless senor network is presented. In penultimate section experimental study is carried out. The conclusion and future work is described in last section.

The research contribution of this work are as follows

- Firstly, this work presented maximize resource utilization based channel access model for UWSNs.
- Presenting a novel cross layer design for cooperative communication (among MAC and physical layer) to detect jammed node and utilizing spectrum efficiently.
- Presenting channel load capacity of authenticated sensor for maximizing resource utilization without affecting adjacent contending sensor device.
- Experiment outcome shows, the proposed MRUCA model attain superior performance than existing model in terms of bit error rate, detection rate, packet sending ratio, and slot utilization considering grid and random topology deployment.

2. LITTERATURE SURVEY

This section present extensive survey on provisioning security and addressing security issues in underwater wireless sensor network and identified research issues to model an enhanced secure and efficient resource allocation model for UWSN. In [19], showed MAC protocol is a key element in UWSN similar to terrestrial network. However, UWSN has unique feature such as, low channel reliability, very small channel capacity, high dynamics of channel quality, and long propagation delay. Thus, MAC design modelled for terrestrial network cannot work well for UWSN. Here they conducted extensive survey of various MAC design proposed in recent times for building enhanced MAC model. Further, major remaining issues and possible research directions are also discussed. In [20], showed for prolonging lifetime of UWSN, two factor such packet size and transmission power plays vital factor. At one hand, smaller packet are more robust to packet error when compared with larger packets. Thus, using smaller packets aid in reducing bit error. However, it requires larger frame for transmission and hence, induce energy and network overhead. For minimizing frame error, transmission power can be increased. However, this will result in unnecessary energy dissipation in the network. Thus, it is important to consider both packet size and transmission power for enhancing lifetime of network. Here, the presented optimization model using integer linear programming to maximize lifetime of network considering both packet size and transmission power. Along with, a realistic link-layer energy dissipation model is presented using physical layer features of UWSNs.

In [21], showed that channel shared among contending sensor device to utilize resource efficiently. However, sharing channel are prone to impersonation and various other kind of attacks [22]. In [21] presented a spatial reuse based resource allocation model for UWSN for avoiding destructive collision. Major cause of such collision is due to near-far effect [18] where sensor device placed faraway from receiver is jammed by a closer sensor device. Here, they considered spatial reuse time-division multiple access (TDMA) for increasing throughput. They adopted both opportunistic and contention free. Their main objective is to guarantee per-node packet transmission rate and maximize time slot (resource) allocation. Their model increases contention free packet transmission, and decrease scheduling delay of opportunistic packets. However, it induces collision among neighboring contending device. In [15], showed that UWSN packets rarely include encryption due to physical and performance limitations. Thus, UWSN is exposed to various kind of security attack breaching legitimate message. Here they presented an algorithm for message authentication in an UWSN environment. Further, observed that an attacker can impersonate the channel associated with the authenticated sensor device only for a single or certain set of receiving sensor device. This is due to strong spatial dependency of the UWSN channel. Considering these observation, they presented a model using cooperative strategy among trusted sensor device toward base station or sink. For each incoming message, the sink fuses beliefs computed by the trusted sensor device to reach an authentication decision. These beliefs are computed by estimating statistical channel parameters, preferred to be the most sensitive to the communicating device movement. Outcome shows accurate identification of an attacker's packet.

In [17], outlined a hybrid design that is composed software defined network, physical layer security, cross-layer design, cognition, node cooperation and context-awareness. They envisioned a security model at both network as well as at the node level that adapt to dynamic environmental condition, the status of the network, and possible wide range of attacks or security breaches. Here they discussed several kinds of attacks, security breaches and countermeasures along with implementation, deployment and functionality issues and challenges of building hybrid security model for UWSN. The main focusses of their model design is to suggest future research direction to research community or organization working on UWSN. In [18], presented topology-efficient discovery model for UWSN. Here they used network information of source and destination sensor device for performing routing and scheduling packet transmission. They aimed to assure better convergence time in completing topology discovery and the network transforms to its steady-state scheduling design. For meeting, they aimed to assess the link reliability and to identify acoustic link. Their method allow sensor device to share time slots while minimizing/controlling the potential

collision to reduce overhead and delay in topology discovery process. Further, it offers power control mechanism among near–far node pairs (NFNPs) to improve spectrum utilization (.i.e. offers spatial reuse). Though, their method offers better spectrum utilization with minimal topology discovery time. However, without proper scheduling and delays in transmissions, many packets still collide.

From extensive survey it can be seen the spatial reuse mechanism has been widely applied across state-of-art method to utilize resource efficiently. However, it induces various security issues. Further, sensor node cooperatively transmit among adjacent sensor device to minimize energy consumption and utilize spectrum resource efficiently. However, these model do not consider physical layer information into consideration. Thus, affecting network performance. Along with, considers scheduling of channel to utilize resource efficiently. However, when user are selfish it incurs collision overhead among adjacent sensor device. Further, very limited work is carried out for detecting reactive jammer. Therefore, there is a requirement for new model that that detect jamming effectively and at the same time utilize resource efficiently. This work present a maximize resource allocation based channel allocation model with presence of jammer node for underwater sensor network.

3. MAXIMIZE RESOURCE UTILIATION BASED CHANNEL ACCESS MODEL FOR UNDERWATER WIRELESS SENSOR NETWORK

This work present Maximize Resource Utilization based channel access (MRUCA) model for underwater wireless sensor network (UWSN) with the presence of jamming sensor device. For maximizing resource utilization without affecting adjacent contending device a channel access model adopting cross layer design (i.e., cooperative communication among physical and MAC layer) is presented. Firstly, the system model is defined. Then, the reactive jamming model adopted for research work is described. Then, the cross layer design of physical and MAC layer is presented. Further, the method for identifying authenticated sensor device is presented. Along with, cross layer based channel access model is defined. Lastly, channel load capacity is estimated to maximize resource utilization using either direct or through hop based transmission.

3.1. System 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 wireless sensor network can be seen as a set of concurrent device-to-device communications. 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.

3.2. Reactive jamming model

Let's consider that there is one 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:

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

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

$$1^U q_k \leq q_k^{\uparrow}, \tag{2}$$

where 1 depicts an $1 * |O|$ vector of '1', and $q_k^{\uparrow}$ is the maximum power of the jammer. Due to the diversity of frequency channels, the jammer must assign its power constraint in a way that aid in attaining good jamming effect.

3.3. MAC layer model

The cooperative (mutual) jamming detection model is designed based on mutual functional computation among physical and MAC layers. In MAC layer, sensor device controls their channel accessible probability to attain higher chances to communicate to devices that are being jammed. For satisfying, an opportunistic spectrum access (OSA) model with adjustable spectrum access probability is required at MAC layer. For such consideration, slotted multichannel CSMA is considered where sensor device can adjust the channel access probability. Our MAC model is similar to state-of-art model (i.e., it is based on

contention) where communication time is divided into set of time slots, and all sensor device is considered to be synchronized. At each time slots, a sensor device at most select only one channel at a time for performing transmission, similar to frequency hopping methodology. However, the channel is arbitrarily selected (i.e., a sensor device select each channel with certain probability). A sensor device is also permitted to select none and in this scenario the sensor devices acts as hop device for other contending sensor device. If a sensor device select channel $g \in G$, it initially sense the channel at the start of the time slots, to decide if the channel is accessible. Contention may arise as there may be multiple contender (sensor device) selecting the same channel. Similar to CSAM, a contending sensor device set arbitrary back off time and initialize counter, and the first device counter turns to zero win the contention for channel access. For easiness and attain negligible collision probability, the contention window is kept feasibly large. The proposed MAC design, allows the sensor device to alter it channel accessible probability by just fine-tuning the channel sensing probability of different channel. Thus, let r_o^g, $g \in G$ depicts the channel sensing probabilities of sensor device o on channel g. Further, the sensor device may induces delay of its transmission for serving as hop device for other senor device due to nonzero probability of sensor device o. Thus we have:

$$\sum\nolimits_{g \in G} r_o^g \leq 1$$

3.4. Physical layer model

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 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.

3.5. Strategy of authenticated sensor device

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. Naturally, the cooperative hoping transmission probability is a function representation of the channel sensing probability r_o^g, of the policies of jammer q_k, and the wireless sensor network topography. The sensor device that decide to sense the same channel by initializing an arbitrary back off and the sensor device with maximum probability will obtain contention for transmission. The feature describing the cooperative transmission at both layers, i.e., channel accessible probability and cooperative hoping probability, are both functional representation of the channel accessible probability, network topography, and for a respective jammer policies. Thus, we can utilize channel accessible probability as the policy space of an authenticated sensor device and can be represented as follows:

$$r_o = \left(r_o^g\right)_{g \in \tilde{G}} \tag{3}$$

with,

$$\tilde{G} = G \cup \{0\} \tag{4}$$

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 condition:

$$r_o^g > 0, \forall o \in O, \forall g \in \tilde{G} \tag{5}$$

$$r_o^g \leq 1, \forall o \in O, \forall g \in \tilde{G} \tag{6}$$

$$1^U r_o = 1, \forall o \in O \tag{7}$$

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

$$r = (r_o)_{o \in O} \tag{8}$$

and similarly, the sensing probability strategy of all user except for o can be obtained as follows:

$$r_{-o} = (r_n)_{n \in O/o} \tag{9}$$

3.6. Channel accessible probability evaluation

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

$$D_o(r, q_k) = \sum_{g \in G} r_o^g \beta_o^g(r, q_k) D_o^g(r, q_k), \tag{10}$$

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. As described above, MAC layer cooperative transmission is attained through stochastic channel access. That is, the sensor device $o \in O$ is able to resourcefully access frequency channel $g \in G$ if session o wins the channel accessible competition and the channel sensed is idle at session$o$'s transmitting sensor device $t(o)$. Let $\hat{\beta}_o^g(r)$ depicted as the probability that session o wins the contention game and $\tilde{\beta}_o^g(q_k)$ be represented as the probability that channel g is idle, the channel accessibility probability $\beta_o^g(r, q_k)$ in (10) can be computed as follows:

$$\beta_o^g(r, q_k) = \tilde{\beta}_o^g(q_k) \hat{\beta}_o^g(r) \tag{11}$$

If we consider q_{th}as power threshold below which a frequency channel is sensed idle, thus $\tilde{\beta}_o^g(q_k)$ can be expressed as follows:

$$\tilde{\beta}_o^g(q_k) = Q\left(q_k^g I_{kt(o)} \cdot \left(i_{kt(o)}^g\right)^2 + \left(\alpha_{t(o)}^g\right)^2\right) \leq q_{th} \tag{12}$$

where $i_{kt(o)}^g$, $I_{kt(o)}$ is the capturing fading and path loss component of the link among jammer and session o's transmitting sensor device $t(o)$ on frequency channel g, respectively, and $\left(\alpha_{t(o)}^g\right)^2$is the noise power. As $i_{kt(o)}^g$ Rayleigh distributed with fading component $\delta_{t(o)}^g$, the $\tilde{\beta}_o^g(q_k)$ in (11) can be rewritten as follows:

$$\tilde{\beta}_o^g(q_k) = \int_0^{y_\uparrow} 1 - f^{-y^2/\delta_{t(o)}^g}\, dx \tag{13}$$

Using (12), $y_\uparrow$ can be computed as follows:

$$y_\uparrow = \sqrt{\left(q_{th} - \left(q_{th} - \left(\alpha_{t(o)}^g\right)^2\right)/\left(q_k^g I_{kt(o)}\right)\right)}. \tag{14}$$

We further compute the probability that a sensor device $o \in O$ wins the medium accessible game post performing sensing the frequency channel $g \in G$ to be idle. Let consider set of sensor device contending with sensor device o on frequency channel g represented as $O_o^g \subset O/o$, the winning probability for sensor device o can be expressed as follows:

$$\frac{1}{1 + \left|O_o^g\right|}$$

where $\left|O_o^g\right|$ is the number of sensor device in O_o^g. Since each probable contending sensor device $n \in O_o^g$ joins the access contention game with probability $r_n^g \tilde{\beta}_n^g(q_k)$, the cardinality of O_o^g, that is $\left|O_o^g\right|$ is considered to be Poisson distributed with mean and is expressed as follows:

$$F\left(\left|O_o^g\right|\right) = \sum_{n \in O/o} r_n^g \tilde{\beta}_n^g(q_k). \tag{15}$$

Then, the cumulated probability of establishing a channel access contention game for sensor device o, that is, $\hat{q}_o^g(r)$ in (11), can be computed as follows:

$$\hat{q}_o^g(r) = \sum_{l=0}^{|O|-1} \frac{1}{1+l} \cdot \frac{\left(F(|O_o^g|)\right)^l f^{-F(|O_o^g|)}}{l!}. \quad (16)$$

3.7. Estimated channel load capacity

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 (10) is computed as follows:

$$D_{o,g}^{direct}(q_k) = C \log\left(1 + \mu_{o,g}^{t2e}(q_k)\right) \quad (17)$$

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

$$\mu_{o,g}^{t2e}(q_k) = \frac{q_o I_o \cdot \left(h_o^g\right)^2}{\left(\varphi_{e(o)}^g\right)^2 + q_k I_{ke(o)} \cdot \left(i_{ke(o)}\right)^2} \quad (18)$$

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 (10) 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 follows:

$$D_{o,g}^{coperative}(q_k) = \frac{C}{2} log\left(1 + \min\left(\mu_{on,g}^{t2s}, \mu_{o,g}^{t2e} + \mu_{no,g}^{s2e}\right)\right) \quad (19)$$

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 (18) and (19) the cooperative capacity can be lower or higher than the direct capacity. This is due to ½ coefficient consideration in (19). Thus, the overall estimated capacity attainable by sensor device o over channel g can be computed as follows:

$$D_o^g\left(r, q_k = \sum_{n \in O/o} D_{o,g}^{coperative}(q_k) + \sum_{n \in O/o} D_{o,g}^{direct}(q_k)\right) \quad (20)$$

Form (20) 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 utility parameter of each sensor device can be expressed as follows:

$$V_o(r, q_k) = \log\left(D_o(r, q_k)\right) \quad (21)$$

and the proposed objective parameter to maximize the resource utilization of sensor device without affecting other legitimate sensor device can be expressed as follows:

$$\begin{aligned} &Given: \ q_k \\ &\underset{r \in (0,1)^{|O|}}{\text{Maximize}} \ V_o(r, q_k) = \sum_{o \in O} V_o(r, q_k) \\ &Subject\ to: (5), (6), (7) \end{aligned} \quad (22)$$

This work present a distributed strategy to meet proposed resource utilization objectives of (22). 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. The proposed channel access model attain superior performance than state-of-art model which is experimentally proved in next section below.

4. SIMULATION RESULT AND ANNALYSIS

This section present experiment analysis of proposed maximize resource utilization based channel access (MRUCA) model with and without presence of jammer nodes and compares the outcome with state-of-art model [18]. For conducting experiment analysis, this work used MAcoSim [23-25]. MAcoSim is operated by both GUI and MATLAB command line interface and is written on top of NS2 simulator. Additionally, centralized parameter manger was employed to acquire easy configuration. The output trace is written in NAM file which can be used later to analyze the simulation experiment. The parameter considered for experiment analysis is similar to [18]. This work considered a topology with 8, 12, and 16 sensor device placed randomly in a region of 16m*16m with one jammer node. Along with experiment are conducted considering topology with 28, 32, and 36 sensor devices placed in grid region of 16m*16m with presence of singe jammer node. Jammer will send 8-bit packet in each time slot and each node will generate traffic (transmit) 3 bit of data. Experiment is carried out considering 100 simulation cycles and the outcome is logged in terms of packet received, contention packet received, amount of packet being dropped, bit error rate, packet sending ratio and bit error rate.

4.1. Packet transmission performance for random topology deployment

Figure 1 shows the packet transmission performance attained by proposed MRUCA model considering with and without jamming considering varied nodes. The outcome shows without any jamming nodes the MRUCA model successfully transmit 101, 112, and 129 packets considering 8, 12, and 16 nodes, respectively. Similarly, with presence of single jammer node MRUCA model successfully transmit 96, 106, and 119 packets. An average of 6.14% packet drop is induced due to presence of jammer nodes considering varied nodes size. Further, experiment is conducted to evaluate the Bit Error Rate (BER) performance. The outcome shows proposed model with presence of jammer attain BER of 0.0204, 0.03636, and 0.0325 for 8, 12, and 16 nodes, respectively with signal to noise ratio (SNR) = 4dB. Figure 2 shows contention packet transmission performance attained by proposed MRUCA model considering with and without jamming. The outcome shows without any jamming nodes the MRUCA model successfully transmit 101, 112, and 129 packets. Similarly, with presence of single jammer node MRUCA model successfully transmit 98, 110, and 123 packets considering 8, 12, and 16 nodes, respectively. A 3.22% packet drop of contention packet is induced due to presence of jammer nodes. From, Figure 1 and Figure 2 it can be seen that without jamming node the MRUCA model attain 100% slot (bandwidth) utilization efficiency. However, with presence of jamming nodes the MRUCA model attains 93.86% slot utilization efficiency.

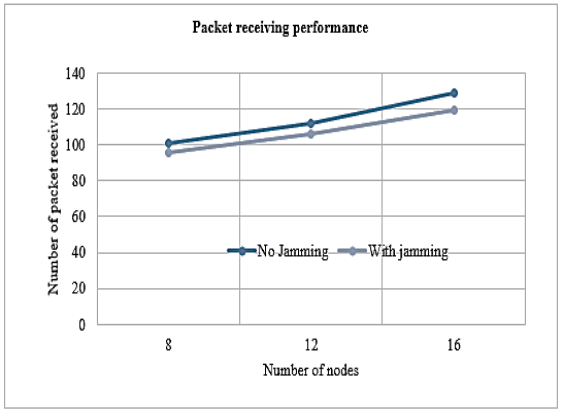

Figure 1. Packet receiving performance

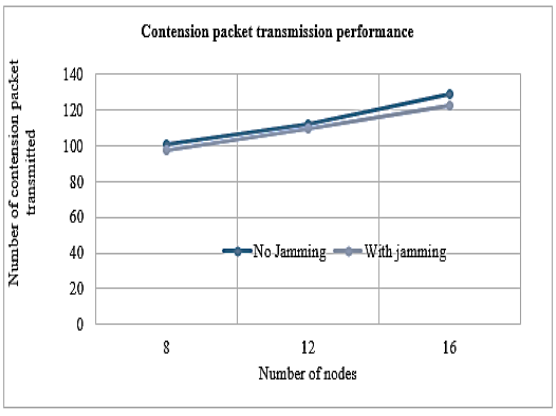

Figure 2. Contention packet transmission performance considering varied nodes

Further, the MRUCA model is evaluated for detecting jamming nodes (packets) and packet sending ratio performance. In Figure 3 the jamming detection performance of MRUCA is evaluated. From figure it can be seen the jammer node induce 78, 82, and 82 duplicate or fake packets in network considering 8, 12,

and 16 nodes, respectively. Out of which is 76, 80, and 78 packet is identified and dropped from the network considering 8, 12, and 16 nodes, respectively. Thus, the MRUCA model attain a detection accuracy of 96.69%. In Figure 4 packet sending ration performance is shown. From result, it can be seen without jamming our model attains 100% packet sending ratio. However, with presence of jammer node, an average of 97.02% packet sending ratio is attained considering varied nodes. From overall result attain it shows that the proposed MRUCA model attain superior performance (less collision) when compared with existing model [18].

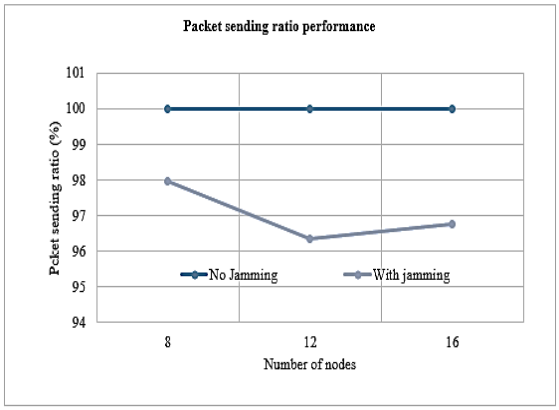

Figure 3. Jamming detection performance considering varied nodes

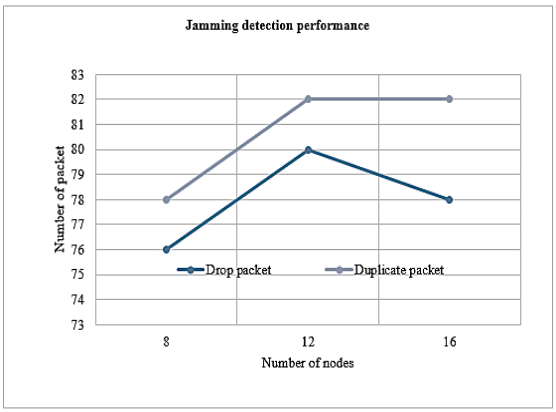

Figure 4. Packet sending ratio performance considering varied nodes

4.2. Packet transmission performance for grid topology deployment

Figure 5 shows the packet transmission performance attained by proposed MRUCA model considering with and without jamming under varied nodes (i.e., 28, 32, and 36). From Figure 5 it can be seen without jammer no packet drop can be seen. However, with presence of jammer it can be seen 25.33 packets been dropped. However, these packet are been corrupted by the jammer node. As a result, are identified and eliminated from network. Thus, will aid in reducing congestion in network. Further, with presence of jammer only 2 packet is been retransmitted. However, in case of no jammer 4.66 packet has been retransmitted. Further, from Figure 6 the proposed model attain 92.26% and 100% packet sending ratio performance with and without presence of jammer, respectively. An average drop or underutilization of spectrum of 7.74% is induced due to presence of jammer nodes considering varied nodes size. Further, experiment is conducted to evaluate the Bit Error Rate (BER) performance. The outcome shows proposed model with presence of jammer attain BER of 0.0588, 0.0588, and 0.0571 for 28, 32, and 36 sensor device, respectively with signal to noise ratio (SNR) = 4dB.

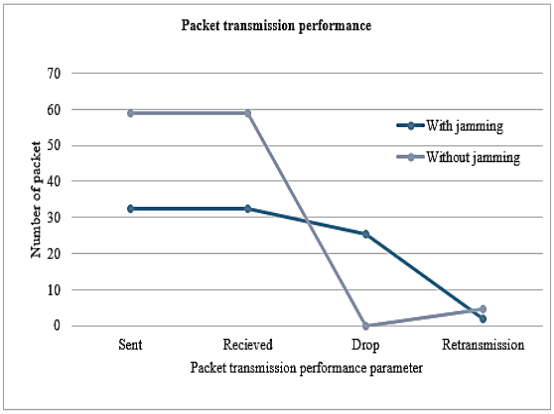

Figure 5. Packet transmission performance for grid environment considering varied sensor device

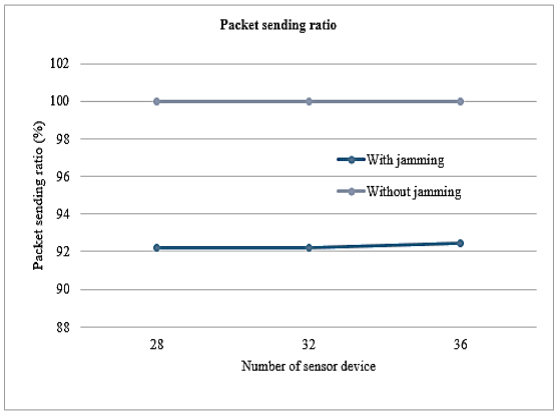

Figure 6. Packet sending ratio performance for grid environment considering varied sensor device

4.3. Result and discussion

This section present performance evaluation discussion of proposed MRUCA over existing model [18]. Table 1, shows result attained by proposed MRUCA over existing model. In [18] evaluated their model using utility function (i.e., slot utilization), near far node pair (NFNP) detection accuracy (i.e., detection rate) and packet collision (drop rate). However, packet transmission performance is not evaluated by them. From overall result attained by existing model shows they reduce topology discovery time. Further, adoption of spatial reuse aided in attaining better resource utilization. However, packet still get collided due to improper scheduling and transmission delay. In other side the proposed model attain better slot utilization, packet drop rate, and detection rate which was experimentally proven above. The significant result attained by proposed model is due adoption of cross layer where the model jointly optimizes the cooperative hopping probabilities and channel accessibility probabilities of authenticated sensor device). Along with channel load capacity of authenticated sensor is estimated for maximizing resource allocation without affecting neighbouring sensor device.

Table 1. Performance comparison of proposed model MRUCA over existing model

	[18]	Proposed MRUCA
Drop rate (collision)	33.33%-57.15%	3.22% to 6.14%
Bit error rate	-	0.204 to 0.0325
Packet Sending ratio	-	97.02%
Detection accuracy	-	96.69%
Slot utilization	90.0%	93.86%

5. CONCLUSION

Firstly, this work conducted extensive survey to identify issues and challenges in designing efficient channel access model under presence of jammer node. Further, identified security and performance venerability of UWSNs with presence of jamming node. Among jamming attack, reactive jamming attack is considered to be very difficult to identify and remove it from the network. Number of approaches has been presented to prevent such attack in UWSN. However, the existing model failed to distinguish between the corrupted and uncorrupted parts of a packet. As a result are not efficient in identifying jamming nodes. Thus affecting network performance (i.e., induce bandwidth wastage). For overcoming research challenges, this work presented maximize resource utilization based channel access model adopting cross layer design. A novel cooperative scheduling mechanism is presented that mitigate jamming nodes and aid in better resource utilization by jointly optimizing the cooperative hopping probabilities and channel accessibility probabilities. Further, for maximizing resource utilization without affecting performance of adjacent contending sensor device a channel load capacity is estimated using either direct or through hop based transmission. Experiment are conducted to evaluate performance of MRUCA over existing model considering both random and grid topology deployment. The outcome shows the MRUCA attains good bit error rate performance with 6.14% and 7.74% packet drop due to presence of jammer nodes considering random and grid deployment, respectively. Similarly, 3.22% contention packet drop is attained due to presence of jammer node under random deployment. The MRUCA attain 97.02% and 93.86% packet sending ratio and slot utilization efficiency, respectively with detection accuracy of 96.69% under deployment. Similarly, under grid environment with presence of jammer model the proposed model attain 92.26% packet sending ratio performance. The overall result attained shows superior performance than state-of-art model. The future work would consider presenting distributed resource allocation scheme to support diverse real-time application under UWSNs.

REFERENCES

[1] W. Aman, M. M. U. Rahman, and Junaid Qadir, "Impersonation Detection in AWGN-limited Underwater Acoustic Sensor Networks," *arXiv:1805.12403*, 2018.

[2] A. Kamaruddin, Md. A. Ngadi and H. Harun, "An Energy Efficient Void Avoidance Opportunistic Routing Protocol for Underwater Sensor," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 4, pp. 1948-1956, 2019.

[3] S. C. Desai, K. S Jagadeesh, and K. D. Dhruve, "Elephant Swarm Optimization for Wireless Sensor Networks-A Cross Layer Mechanism," *International Journal Of Computer Engineering & Technology (IJCET)*, vol. 4, no. 2, pp. 45-60, 2013.

[4] O. A. Osanaiye, A.S. Alfa and G.P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 6975-7004, 2018.

[5] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming Sensor Networks: Attack and Defense Strategies," *IEEE Network*, vol. 20, pp. 41–47, 2006.

[6] M. Wilhelm, I. Martinovic, J.B. Schmitt, and V. Lenders, "Short Paper: Reactive Jamming in Wireless Networks-How Realistic is the Threat?," in: *Proc. of WiSec, Hamburg, Germany*, pp. 47–52, 2011.
[7] M. Strasser, B. Danev, and S. Capkun, "Detection of Reactive Jamming in Sensor Networks," *ACM Trans on Sens. Netw*, vol. 7, no. 2, pp. 1-29, 2010.
[8] K. Pelechrinis, M. Iliofotou and S.V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Commun. Surv. Tutor*, vol. 13, no. 2, pp. 245–257, 2011.
[9] S. Misra, S. Dash, M. Khatua, A.V. Vasilakos, and M.S. Obaidat, "Jamming in Underwater Sensor Networks: Detection And Mitigation," *IET Commun*, vol. 6, no. 14, pp. 2178-2188, 2012.
[10] D. Giustiniano, *et al.*, "Detection of Reactive Jamming in DSSS-Based Wireless Networks," in: *Proc. of WiSec, Budapest, Hungary*, 2013.
[11] M. Khatua, 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, TIFR, Mumbai*, pp. 118-132, 2013.
[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.
[13] S. Neelambike, and J. Chandrika, "An Efficent Distributed Medium Access Control for V2I VANET," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 9, no. 3, pp. 742-751, 2018.
[14] P. Bhavathankar, S. Subhadeep, 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.
[15] R. Diamant, P. Casari, S. Tomasin, "Cooperative Authentication in Underwater Acoustic Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 954-968, 2019.
[16] 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.
[17] 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, 2017.
[18] Buddesab, Thriveni, Venugopal K R, "Trust Model Genetic Node Recovery Based on Cloud Theory for Underwater Acoustic Sensor Network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3759-3771, 2019.
[19] J. Youngjun, and L. Sangsoon, "Design and Implementation of Heterogeneous Surface Gateway for Underwater Acoustic Sensor Network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 2, pp. 1226-1231, 2019.
[20] 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, 2019.
[21] 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, 2017.
[22] S. K. Pushpa, S. Ramachandran, and K. R. Kashwan, "A Novel Skeleton Extraction Algorithm for 3d Wireless Sensor Networks," *Global Journal of Computer Science and Technology*, vol. 13, no. 16-E, 2013.
[23] Anjana P Das, and S. M Thampi, "Simulation Tools for Underwater Sensor Networks: A Survey," in *Network Protocols & Algorithms*, vol. 8, no. 4, 2016.
[24] S. Y. Kang, M. Aldwairi, and Ki-ll, Kim, "A Survey on Network Simulators in Three-Dimensional Wireless Ad Hoc and Sensor Networks," *International Journal of Distributed Sensor Networks*, 2016.
[25] "Macosim: Matlab-based acoustic underwater simulator," [Online]. Available: http://www.sit.iitkgp.ernet.in/smisra/swan/tre/macosim.html, [accessed on 15-Dec-2016].

BIOGRAPHIES OF AUTHORS

Sheetal Bagali received her B.E in Electronics and Communication in 2007 and M.Tech degree in VLSI & Embedded System 2015 from VTU and pursuing Ph.D. degree in in Underwater Communication from VTU. Currently she working as Assistant Professor at Sir MVIT, Bengaluru. Over all Teaching experience is 6 years. Her research interests include Acoustic communication, Communication systems and Low power VLSI.

Dr. R. Sundaraguru received AMIE in E&C in 1993, M.E in Communication systems in 1997 at Thiagarajar College of Engg. Madurai and Ph.D. in wireless communication from Anna University Chennai. He is currently working as professor and Head in the department of ECE, Sir MVIT. He has around 3 years of industrial experience as service/assistant engineer and around 21 years in teaching. His area of research includes wireless communication, Image processing, Networking, VLSI and Embedded systems. To his credit, he has published paper in reputed International journals and IEEE Conferences, about 7 papers in International Journal and 15 paper in National and International conferences. He has coordinated number of Faculty development programme. Guided more than 75 UG and 30 PG projects. He is a member of different professional bodies like Institute of Engineers, Member of IETE and ISTE. Email: sugursg@sirmvit.edu