A Novel Cooperative Model Using Game Theory for Efficient Routing in Underwater Acoustic Sensor Networks (UASNs)

Dalhatu Muhammed[1], Abubakar Ibrahim[2], Abubakar Ahmad Aliero[1], Abdul-azeez Muhammad Bello[3]
[1]Department of Computer Science, Kebbi State University of Science Technology, Aliero
PMB 1144 Birnin Kebbi, Nigeria
[2]Asset Management Department (AMD), Nigeria Deposit Insurance Corporation (NDIC) No. 15 Marina, Lagos, Nigeria
[3]Center for Information Technology, Waziri Umaru Federal Polytechnic Birnin Kebbi. Kebbi State Nigeria
E-mail: dmaliero@yahoo.com, ibrahimab@ndic.gov.ng, abbatee4u@yahoo.com, abdulshamaki@gmail.com

Abstract— The emergine of the recent techonology over the last few decades' years' researchers focus on the full exploration of Underwater potentials and resources with the help of this imaging technology sensor networks; Reliable packet routing in Underwater remain unexplore. Sensor nodes are deployed in the Underwater environment for many different sensing and routing applications. However, the different features of underwater such as channel failure, higher mobility of the nodes and presence of malicious node makes reliabe cooperative routing among sensor node a great challenge and providing reliable cooperative routing in Underwater Acoustic Sensor Networks become necessary to eliminate the issue of higher packet dropped mainly caused by malicious nodes. This research work proposed A Novel Cooperative Model Using Game Theory for Reliable Packet Routing in Underwater Acoustic Sensor Networks (UASNs) using Dynamic Bayesian Game which incooperate belief, trust and motivation, developed algorithms for finding the most suitable strategy for a player and best response for providing reliable cooperative packet Routing in UASNs. The proposed cooperative model (Proposed CM) was implemented in underwater simulator Aqua-Sim and evaluated with some related works based on propagation delay, packet delivery ratio, transmission overhead and transmission latency. Our simulation results reveal that our proposed CM achieve better performance over the existing schemes.

Index Terms— Belief, Cooperation, Efficient Routing, Game Theory; Motivation, Trust and Underwater Sensor

1 Introduction

Generally, water covers seventy percent of the earth's surface, where vast amount of unexplored resources lies there over the last few years. With the Recent development in sensor network and emerging underwater acoustic sensor network (UWSN), made the development of underwater application feasible. The importance of underwater application is attracting the attention of researchers which lead to the rapid growing of research within various areas in UASNs [1, 2]. Recently, many researchers are now focusing on how to develop varieties of underwater applications to support the lives of living organisms in underwater and even those that are living on the earth surface by the use of collaborative, cooperative and frequent monitoring of underwater environment [3]. Frequent occurrence of disaster in the last few years such as sinking of USS, Kursk submarine disaster Russia and oil leak in golf of Mexico [4-8] have encourage several research teams to carry out research in various oceanic monitoring applications of UASNs such as environmental monitoring, chemical exploration, scientific, military applications, and safety security application need [3].

Similar to any sensor networks exchange of information is a primary important in communication networks and it can be achieved among the nodes in a predefined area coverage or even outside the predefined boundary using a gateway device (sink). In these regards cooperative communication for providing reliability in packet routing for UASNs remains unexplored [1, 9]. In contrast to electromagnetic and optical signal, sound is the best in travelling through the water and Acoustic signal is a sound signal waveform for underwater applications, which is usually produced by sonar. [1]. In UASNs, sensor node is wirelessly interconnected with one or more underwater sink (uw-sink) via acoustic link. These underwater sink are responsible in relaying the sensed data collected from the sensor nodes situated in a particular location in the ocean to the surface station [10, 11].

Each underwater sinks are mainly equipped with some forms of transceivers such as horizontal transceiver, which is use by underwater sink for communicating the configuration data and commands with sensor node (uw-sink to sensor) and also collect the sensed data (sensor to uw-sink). Vertical transceiver is used by uw-sink for relaying the collected data to the surface station. Since the ocean can be as deep as 10km, the range of vertical transceiver must be longer than the horizontal transceiver as it is use in deep water applications [10]. Parallel number of communications are usually occurred in a multiple form from the sinks that are deployed, therefore to handle these issues the surface station has been equipped with an acoustic transceiver. It can also communicate to the onshore sink (os-sink) or surface sink (s-sink) using longer range of the radio frequency (RF) or satellite transceiver. Uw-sink can be

connected with sensors node in two methods either through the direct links (DL) or through multi-hop (MH) path [10, 12]. There are a lot of challenging factors which characterize the unique features of UASNs. These factors are:

Before the recent technology sensor nodes are usually battery powered and these batteries are energy constrain and usually not rechargeable[13], The propagation delay of acoustic channel is five order of magnitude greater than RF in terrestrial channel due to low speed of sound which is 1500m/s, The bandwidth is limited and mainly depend on the distance as a result of high transmission loss with high frequencies and also high environmental noise with low frequencies, Nodes are prone to failure due to corrosion and fouling, Fading and multipath problems makes the acoustic channel impaired severely [14, 15] and Formation of shadow zone due to the high number of bit error rate (BER) and temporary loss of connectivity in a region where the reception of underwater signal is impaired as a result of fading and multipath.

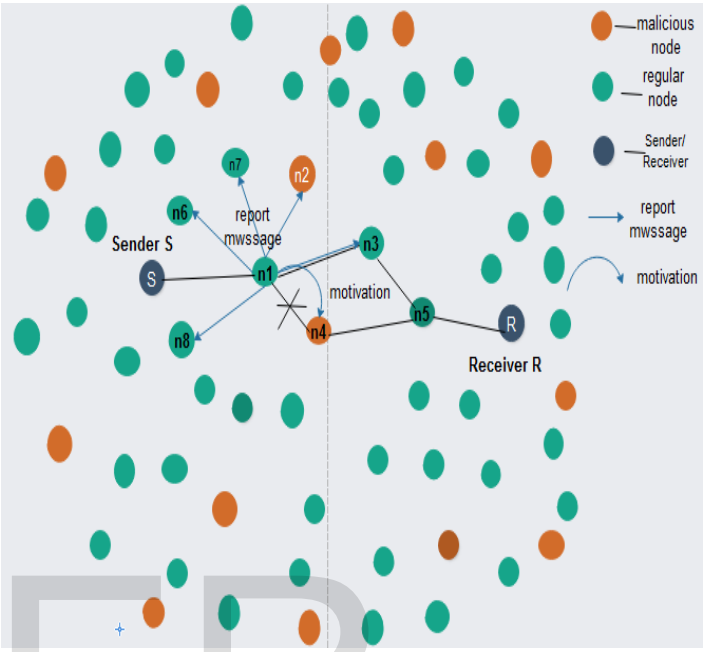
Recently, many researcher have demonstrated interest in exploring the promising features of UASNs[14, 16]. There are many challenging issues that contribute to the UASNs performance degradation that are include high energy consumption, loss of connectivity, security, routing and cooperation [17, 18]. Many applications such as environmental and pollution monitoring, oceanographic data collection, distributed surveillance, oceanic sampling, offshore exploration, disaster prevention, mine reconnaissance among others are developed, however, underwater acoustic senor (UASNs) applications are not well investigated compare to others. [14, 17, 19-21].

Authors in [10, 14, 17, 19] stated that "Applications of UASNs are broadly classified into two categories based on the time duration required, namely i) Long term Aquatic Monitoring (e.g. marine biology, oil/gas monitoring deep sea archaeology, seismic prediction etc.) and Short term Aquatic exploration (e.g. natural resources discovery, anti-submarine mission, lost treasure discovery etc.)". UASNs comprise of tiny sensor nodes capable of sensing, processing and communicating the sensed data to the appropriate destination which are deployed in underwater for an effort in backing vast range of applications in a collaborative monitoring tasks [14, 15].

Cooperative packet routing for UASNs remain a challenging concept due to its unique features, in which some of the protocols designed for MANET and WSN cannot be directly adopted to the underwater environment. Authors in [22, 23] propose a cooperative communication for UWAC by investigating physical layer aspect in cooperative transmission technique for future UWAC system. Researchers in [24, 25] conducted an analysis for error propagation in underwater cooperative multi-hop communication where they examined the expected gains of multi-hop communication. This cooperative communication (packet routing) in UASNs usually occurred between a sender and a receiver where a sender would send a packet to the receiver (target destination). A clear illustration of this process can be obtained in Figure 2 shown below.

Figure 1: A Scenario with 68 nodes with 15 malicious nodes [30-32]

The concept of Game theoretic approach proposed by [26]



analysis reputation system on the basis of incentives cooperation between nodes and a system of price-based. GTBA (Game Theory Based Analysis) proposed by [27] which is an incentive based cooperative method designed to solve the cooperation issues among regular node and malicious node. However, GTBA did not considered several attacks such as malicious node attack which make it not suitable for UASNs. In [28, 29] they proposed a routing protocol for a secure routing in which they utilize the primitives cryptographic concepts for the UASNs mobile nodes and fixed nodes. In [30] they proposed SRPDBG (Dynamic Bayesian Signalling Game model) for enhancing the routing security achieving a successful packet forwarding among nodes involve where they analysed regular nodes and malicious nodes. However, their approaches did not address cooperative mechanism for end-to-end packet delivery in underwater acoustic sensor networks.

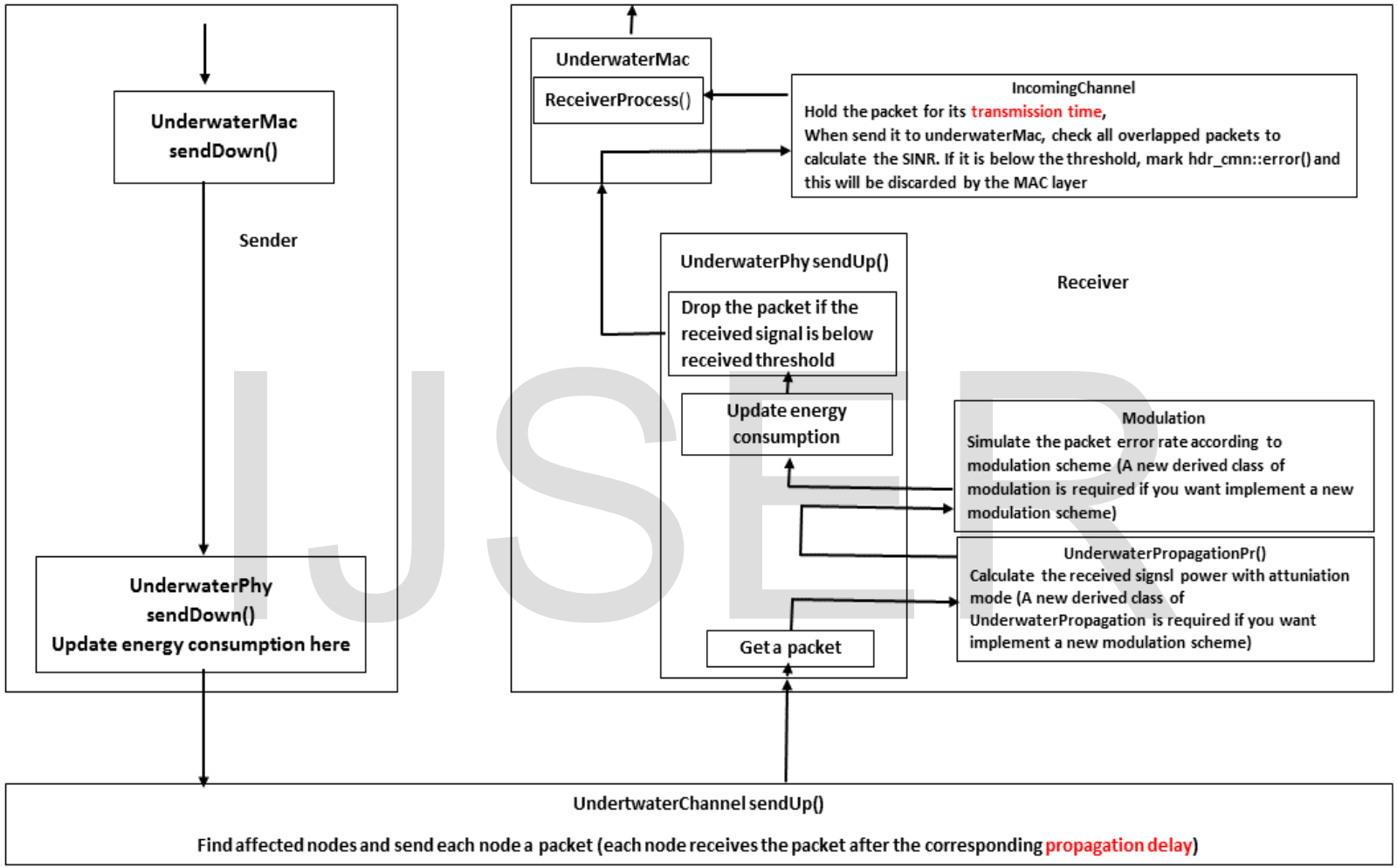


Figure 2: Sender and Receiver Communication Structure in UASN

In this scenario node S want route the packet to node R. Node S chose to route the packet to node n1 as a relay which is inside the routing vector toward the destination and n1 initially route the packet to the n4 and it happen that n4 is a malicious node and n4 dropped the packet. Node n1 notices that n4 is malicious node, thus n1 report to all their neighbors that n4 is malicious and n1 select n3 as a forwarding node which relay the packet to R (destination) [30]. Figure 2 illustrates how malicious node affect the performance of UASN cooperation

Major contributions of this work are i. We propose a cooperative model using game theory for providing reliable cooperative packet routing in UASNs. ii. We studied various strategies used for UASNs cooperative packet routing and developed algorithms for finding the most suitable strategy for a player and best response for providing reliable cooperative packet routing in UASNs. iii. Our proposed CM used Belief, Trust, and motivation for encouraging malicious nodes to participate in packet routing activities which increased packet delivery ratio, decreased delay, decreased transmission overhead and transmission latency. iv. Also, we used the game tree to determine the probability distribution of each player type, the behavior of a player, action of a player and utilities of a player. The remaining parts of this paper are outlined as part 2 Related works, Methodology and Implementation in part 3, Result in analysis and discussions in part 4, conclusion, open issues and research direction in part 5.

2 Related works

The concept of Game theory is a well-developed field of mathematics which is a suitable way of analysing outcomes of group behavior with the basic that players are rational. A rational player chooses an action that maximizes their outcome given their believe about other players' preferences. The game analysis predicts the final outcome when rational players play against rational players. They provides information and instructions to determine the attacks and hence they are unable to provide concreate solutions to the identified problems [33-39].

In [40] authors analyses various approaches of game theory and their impact on network security applications. They provide solution to vast number of problems in network security based on an approach on the theoretic concept of games. Authors in [36, 41] classified and categorized various number of attack strategies against UASN. According to [42] "reputation based Bayesian game is type of game described as a non-zero sum game where players can compute payoffs for each action based on reputation and estimated degree of the opponents."

Authors in [30, 43, 44] proposed enhanced secured routing scheme using a concept of Signalling Game in Dynamic Bayesian model in which they analyse the regular strategy profile of malicious node and how to protect the node from anonymous behavior. Authors in [41] proposed a Distributed Reprogramming Secure and Protocol (SDRP) which uses cryptography identity-based to reduce the storage requirement and communication of every node based on secure reprogramming. A convergence in terms of true cooperation for Bayesian game was designed by [42], which uses the concepts of reputation values to analysed the payoff for the game. They define two different types among the number of participants namely type honest and type dishonest. They illustrate the sustainability of true cooperation based on repeated game even on the dynamic application and there is increase in the average players' reputation over a given time in a certain coverage.

routing modelling with the concepts of dynamic Bayesian game was proposed by [45] in which they analysed routing concepts theoretically to fill the gap between decision making of non-simultaneous and information history which is also incorporated in the process of theoretically routing modelling in the approach of game theory. However, the problem with this approach is it does not provide the practical test of different functions of utilities and the probability distribution in the game on different parameters of networks such as node mobility rate and selfish node in order to have fair comparison with existing works. A scheme for secure and robust routing is proposed by [2, 46], where an interaction among sender node and receiver node was modelled on the basis of game model where a dynamic Bayesian game were used based on node opinion about a the opponent in which the destination node established the mechanism of acknowledgement for the reception of the packet from a participating nodes in the game.

Jiang et. al., [47] propose a scheme based on the game theory of interaction, coding theory and establishment of trust for the restriction of attacks and colluding. In these scheme, the message availability is guaranteed whenever there exists a legitimate path. This scheme also shows that it has achieved efficiency in term of latency, energy consumption as well as availability, but the scheme does not provide reliability of message delivery among nodes. [48] introduced cooperative modelling of selfish behaviors of the node and malicious behaviors of the individual node for a preservation privacy trajectory using a theoretic concept of Bayesian game in which they model the cooperative behavior of selfish (non-cooperative) node and malicious behavior. They analysed and formulate a trajectory form of game in privacy preservation within peer of nodes for a dynamic and strategic form where they used the concept of equilibrium for the evaluation of users' degree of participant strategic trust of TPP game theoretically. However, this scheme does not support

multi-layer game and does not evaluate the plyers payoff hence, the method neither observe attacker nor prevent/motivate the attack.

In [49] Jin et al, study, analyse and addressed vast number of privacy and security problems for different applications in computer science such as mobile and network application, where they organized their works into several modules in which all the module addressed a particular problem in the aspect of security. They also designed a mechanism for security and conducted an analysis in equilibrium, where they highlight advantages and the disadvantages of game theory. However, these work is only covers the theoretical part which is helpful in term of developing solution to the problem of security aspect of the network using an approach of game theory [50]. An access based on point pricing modelling for dynamic game proposed by [51], where they modelled a two-person game between the access point owner and client, in which both have some set of symmetric information. Where the client has information more than the owner of the access provider. It is found that a client has a utility function which is the web browser and is the Nash equilibrium which enables the provider to take advantage of the client and change the constant price charge for the client for a given unit of time. Although majority of the security game classes define a two person strategic games where one of the player would act as an attacker trying to hack and damage the system in order to degrade the system performance or comprise the data packet and the opponent player act as a defender trying to prevent any forms of attack from the attacker. In this study, the game is different due to the fact that the game is an n-person strategic game, where all the players are rational and these players always preferred to take actions that would benefit them [25]. This class of game is the most suitable for maximizing cooperation in UASNs since player must cooperate with his opponent to obtain maximum payoff (utility). The degree of cooperation among the players is always equal to the degree of their payoff. Therefore, the more players cooperate the degree of payoff would be more and vice versa. All the players of this game are assumed to be rational and they only focus in maximizing their expected payoff at all the times.

3 METHODOLOGY

The research methodology plan shown in Figure 3 highlighted the steps taken and procedure followed in achieving the goal of this research, Tie 1 of Figure 3 describe the first steps taken toward the achieving the goal of this research. The second steps (Tie 2) of this research the proposed cooperative game model were designed and implemented based on Trust Strategy-based Dynamic Bayesian Game (TSDBG) and motivation in which the proposed game model comprised of three separate domain where the first domain describe the secret information of player (Sender Si ∈ S) which the opponent player does not have knowledge about this information, Likewise the second domain describe the secret information about the Receiver (Relay) Ri ∈ R which remains as secret as the start of the game. The third domain S and R Actions domain described the two players' interactions which resulted in cooperation among the players where each player selected the best actions which enabled them to get the best response from their opponent and obtained their payoff based on their choices of their domain and the action they selected from the action domain. Furthermore each player evaluate their trust and update their belief about their opponent player, where these three domains can be obtained in Figure 4. Implementation and evaluation would be discussed in the subsequent part

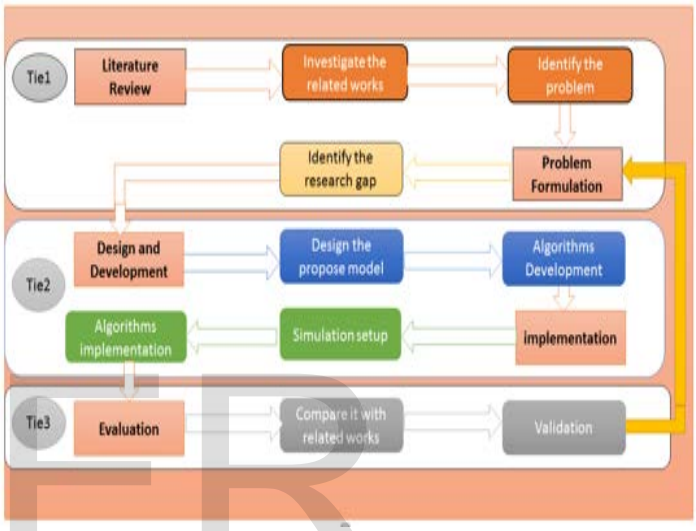


Figure 3: Research Methodology Plan

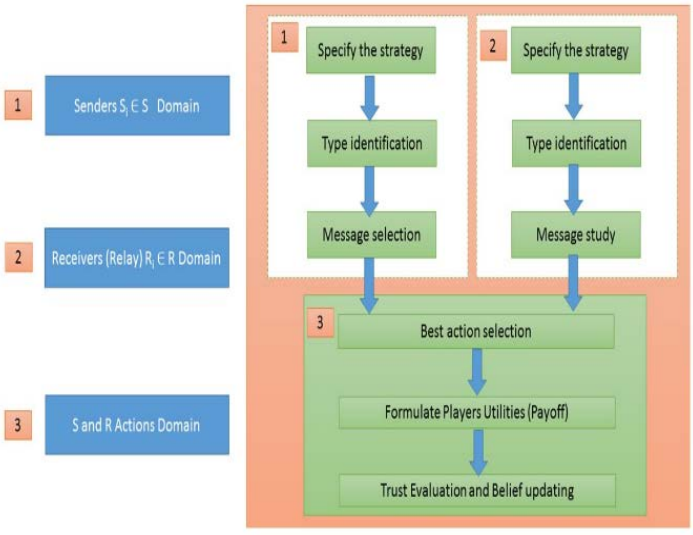


Figure 4: Proposed Game Model

How the Proposed Game Work

In this game, the Trust Strategy-based Dynamic Bayesian Game of incomplete information S-R games where Si refers to the set of Senders $S_i \in S = \{S_1, S_2, S_3, S_4, S_5, \ldots\ldots\ldots\ldots S_n\}$ and Ri refer to the set of Receivers $R_i \in R = \{R_1, R_2, R_3, R_4, R_5, \ldots\ldots\ldots\ldots R_n\}$ where i≥1 and is equal to 1, 2, 3, 4…. n. Each player will select his type from the type strategy space Θ = {Regular, Misbehave} every player will choose an action to perform depending on the number of actions that are available to him in the action space. A Sender Si ∈ S will choose an action to send a message $m \in M = \{m_1, m_2, m_3, m_4, m_5, \ldots\ldots\ldots\ldots m_k\}$, ∀ Si ∈ S ∃ m ∈ M: P (Si ∧ Θ) to the Receiver. The Receiver Ri ∈ R = {R1, R2, R3……Rn} will observe the received message m and perform an action by selecting the available action a in an action strategy space $a \in \boldsymbol{A}$ = {Cooperate (C), Deny (D)} to acknowledge the received of the message. When the Sender Si received the acknowledgement message from the destination node the Sender Si decide which action is to choose t from the action strategy space t ∈ T = {Trust (T), Motivate (Ɱ)} whether he should Trust or Motivate the Receiver Ri on its action and this expression can be obtained in Figure 5. The target of each player is maximizing their outcomes, and with regard to these they will select the most suitable strategy based on their beliefs on their opponent players strategies, though the charges and benefits of a player rely upon the strategies of the opponent players. This game theory is helpful in order to determine the optimal players. The primary target of the sender node or the relay (intermediate) node is to forward the packet generated or received to the destination reliably as soon as possible.

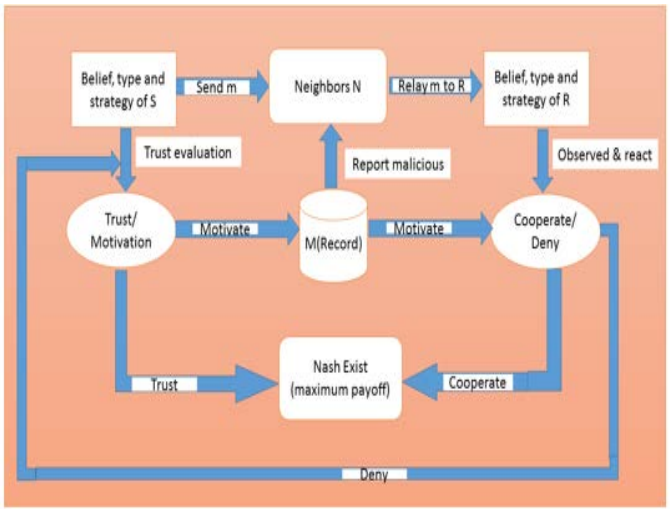


Figure 5: Breakdown of proposed game model

Algorithm 1

Input = message strategy space $m \in M = \{m_1, m_2, m_3, m_4, m_5, \ldots\ldots\ldots\ldots m_k\}$ in PBE

Sequence of algorithm

Let the belief of Sender and Receiver be $\boldsymbol{u}$ and $\boldsymbol{v}$ respectively and let the strategy profile be ω^* and for Sender and Receiver be $\omega_1{}^*$ and $\omega_2{}^*$ respectively and the Trust value of both players is v and this trust values of neighbor nodes can be found in Table 1 which shows the level of trust a node can ascertain to his opponent player based on their interaction.

1. Input $m \in M = \{m_1, m_2, m_3, m_4, m_5, \ldots\ldots\ldots\ldots m_k\}$; // message to be send by player i.e Sender S
2. Determine of $\omega_1{}^*, \omega_2{}^*$; // Determining the type of strategy used by a player based believes and their actions
3. Find payoff for S, R; // To find the gain of each player either Sender S or receiver R
4. If Payoff >= Default value // Compare the gain a player obtained in 3 above with trust value in table 1
5. {Determine $\boldsymbol{A}$}; // Determining the expected actions to be taken by a player
6. end if
7. If $\boldsymbol{A}$ = Cooperate (C) // if the player cooperate
8. {Determine $\boldsymbol{\theta}$}; then go to 12 // The player is regular player
9. Else $\boldsymbol{A}$ = Deny (D) // The player need to be motivated and compare the motivation level with threshold
10. Motivate the node; then go to 15
11. end if else
12. For each ($\boldsymbol{\theta}$ = Regular) do
13. Forward m; then go to 18 //Regular nodes usually forward their message and message from others
14. end for // End For Loop
15. If (motivation>= Threshold) // Level at which the node should be reported as malicious
16. Send alert $\boldsymbol{\theta}$ is Malicious // Alerting the Neighbour nodes on the existence of malicious node
17. end if // End if statement
18. Output = optimal trust solution //To have an optimal trust among the participating nodes
19. Stop. // End

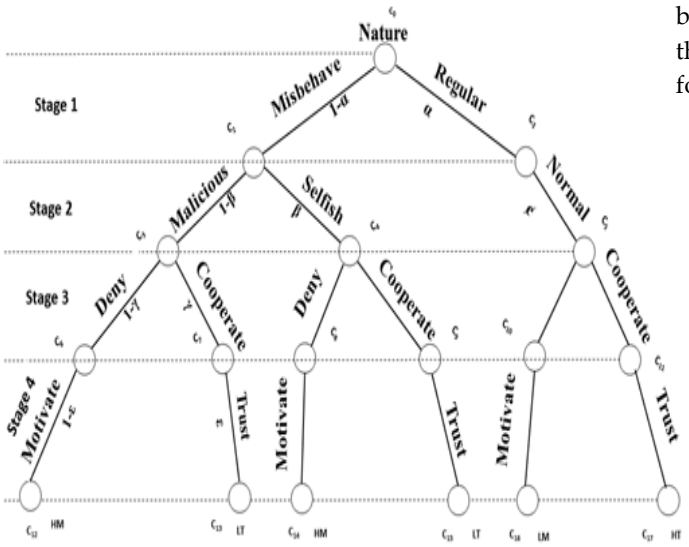


Figure 6: Game Tree

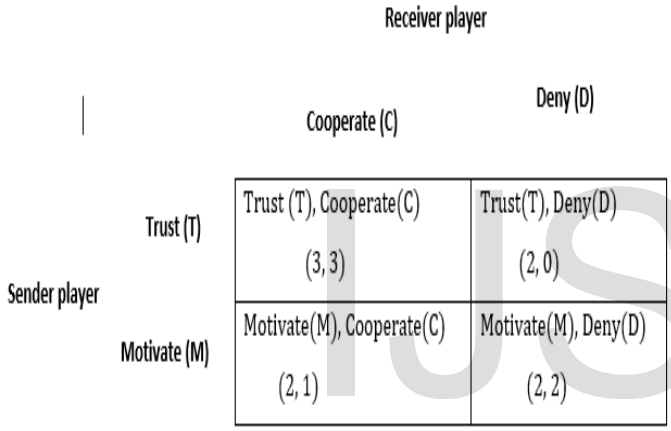


Figure 7: Game Payoff Matrix

Here is a breakdown of the stages involved in the game tree (i.e. stage 1-4) as shown in Figure 6. Which describe the pattern of the game and the probabilities of each player being a Regular or a Misbehaving node as shown below: In Stage 1:

Let the probability of the Sender node is Regular be

$$\Pr(S_i) = p \forall S_i \in S \quad (1)$$

Then, the probability that a Sender node is a Misbehaving node is giving by the

$$P_r(R_i)=q \forall R_i \epsilon R \quad (2)$$

Similarly, if the probability of a Receiver is Regular is

$$P_r(S_i)=1-p \forall S_i \epsilon S \quad (3)$$

Then, the probability of Receiver is Misbehaving nose is

$$\Pr(R_i) = 1-q \forall R_i \in R \quad (4)$$

Also, let the probability of either a Sender Si is Regular or a Receiver Ri is Regular be equal to a which implies that combining Eq. (1) and Eq. (3) we obtained Eq. (5) as follows:

$$\Pr(\alpha) = \Pr(S_i) \cup \Pr(R_i) \Rightarrow p \cup q \forall R_i \in R \,\&\, S_i \in S \quad (5)$$

Similarly Let the probability of either a Sender Si is Misbehaving or a Receiver Ri is Misbehaving be equal to 1-a, therefore combining Eq. (2) and Eq. (4) we obtained Eq. (6) as follows:

$$\Pr(1-\alpha) = \Pr(S_i) \cup \Pr(R_i) \Rightarrow (1-p) \cup (1-q) \forall R_i \in R \,\&\, S_i \in S \quad (6)$$

Stage 2:

If the Sender Si or the Receiver Ri is Regular, then the probability that Si or Ri is would behave Normal is

$$\Pr((S_i \cup R_i) \cap ¢ = 1 \quad (7)$$

Similarly, if the Sender Si or the Receiver Ri is Misbehaving, then he would be either selfish or malicious which is equal to $\beta \vee \beta$-1 respectively, then

$$\Pr(\beta \cup \beta - 1) = 1 \quad (8)$$

Stage 3:

If the Receiver Ri is either Selfish or Malicious, the probability that he would Cooperate (C) is giving by

$$\Pr(\gamma) = (\beta \cup \beta - 1 \cup ¢) \cap C \quad (9)$$

Similarly, the probability that the Receiver Ri would Deny being it either Selfish, Malicious or Normal (D) is giving by

$$\mathbf{Pr(1-\gamma) = (\beta \cup \beta - 1 \cup ¢)} \quad (10)$$

Stage 4:

The probability that a player is Regular, Normal and Cooperate is to combine Eq. (5), (6) and (7) we are going to have

$$\Pr(\varepsilon) = \alpha \cap ((S_i \cup R_i) \cap ¢) \cap (\beta \cup \beta - 1 \cup ¢) \cap C \quad (11)$$

Similarly, the probability that a player is Regular Normal and Deny will be obtained from Eq. (5), (6) and (10)

$$\Pr(1-\varepsilon) = \Pr(\alpha) \cap ((S_i \cup R_i) \cap ¢) \cap \Pr(1-\gamma) \quad (12)$$

Let the probability that the player is Misbehaving, Malicious or Selfish and Cooperate be equal to $\Pr(\varepsilon)^*$ by Eq. (6), (8) and (9)

$$\Pr(\varepsilon)^* = \Pr(1-\alpha) \cap \Pr(\beta \cup \beta - 1) \cap \Pr(\gamma) \quad (13)$$

Likewise, Let the probability that the player is Misbehaving, Malicious or Selfish and Deny be equal to $\Pr(1-\varepsilon)^*$ by Eq. (6), (8) and (10)

$$\Pr(1-\varepsilon)^* = \Pr(1-\alpha) \cap \Pr(\beta \cup \beta - 1) \cap (1-\gamma) \quad (14)$$

Finally, if Eq. (11) moreover, Eq. (13) are satisfied such a player should be Trusted else if Eq. (12) moreover, Eq. (14) are true the player should be motivated.

Table 1: Neighbor Nodes Trust Values [43]

S/N	Trust Value	Description

1	0	No trust at all
2	1	Fairly Trust
3	2	Default Trust
4	3	Fully Trust

The Nash Equilibrium known as (Bayesian Nash Equilibrium (BNE) in TSDBG) of every cooperative games is usually a coalition or a vector in the game matrix from an interaction between two players where both players attained a maximum payoff. In this research the BNE of the game can be obtained from Figure 7 where the sender player chose to trust the receiver and receiver chose to cooperate with the sender and they all obtained a payoff for Trust (T) and Cooperate (C) as (3, 3) and Motivate (M) deny (D) as (2, 2) for sender and receiver respectively, but (T, C) has a maximum payoff of (3, 3) which means that the Nash Exist.

Algorithms Implementation in Aqua-Sim and Simulation Setup

In this research Aqua-Sim-1.0 packets were used as illustrated in Figure 8 below which contains an underwatersensor folder inside this folder, there are five different folders namely uw Mac, um common, uw routing, uw Tcl and uw mobility patterns. In Aqua-Sim all implementation are based on the procedures of object-oriented design where algorithms are implemented in C++ as classes. Each of these folders further divided into sub-folders accordingly, uw common comprise of folders related to underwatersensornode which was derived from the class mobile node in ns2 with some additional functionalities such allowing 3 dimensional deployment of sensor nodes.

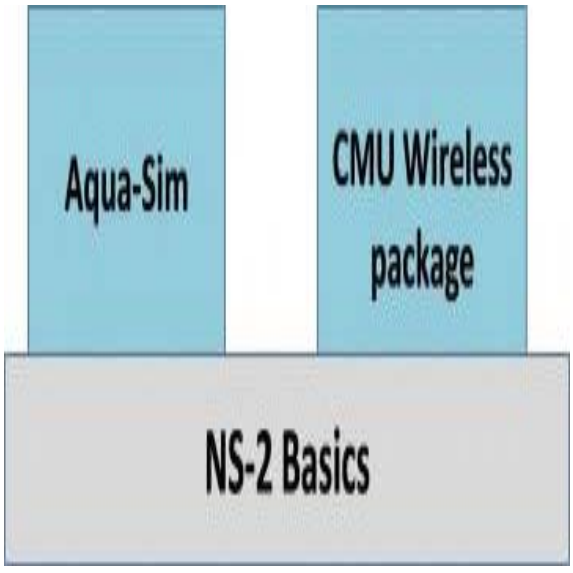


Figure 8: Comparison of Aqua-Sin and CMU Wireless package

Uw sink which is use for vector based forwarding (VBF) and hop-by-hop VBF (HH-VBF) and uw sink vbva which is used for vector based void avoidance (VBVA). HHVBF protocol wsa adopted which similar to any hop-by-hop protocol based on vector forwardin principles, a vector forwarding approache concerned with only nodes that are presrnt in a particular bector region, as illustrated in Figure 9 shown below.

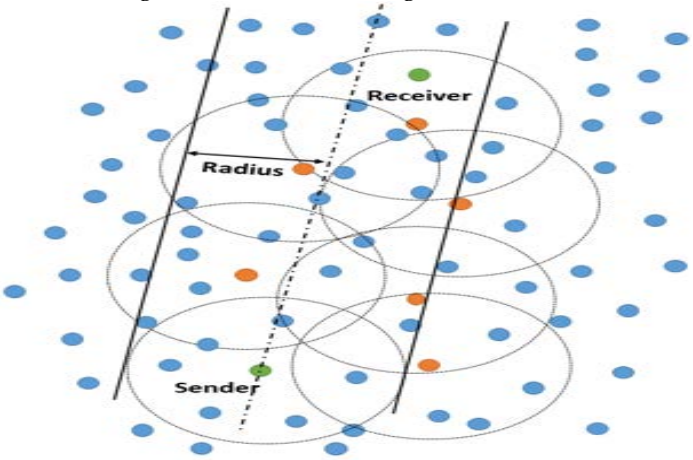


Figure 9: Hop-by-Hop Vector Based Forwarding Protocol

A Tcl script was written which has been used in executing and running the implemented algorithms; all parameters declaration has been made in the Tcl script according to the UASNs declaration specifications. This Tcl script has been run through the terminals awhich generated three main traced information, data files with extension of (.data) which contains all the available data of the running algorithms, NAM files which contain all relevant data related to the physical activities of all the participating node in the topology of this research, a NAM file with extension of (.nam) would run to view the physical appearance of the entire network structure which captured all the data related to network animation. Trace file captured and stored a particular data according to the algorithms and configuration specification, this trace file with an extension of (.tr) normally depend on the designed specification of particular algorithms. All the files described above keep on updating each time a particular Tcl script was run, the content of those files will be automatically updated whenever the scripts is run. This script is run from the terminal using the command (Command line). The Figure below is an Aqua-Sim architecture which presents the process of communication in UASNs ranging from routing protocols, MAC protocols and underwater channel.

The simulation experiment of this research has been implemented in Aqua-Sim simulator based on random generated UASNs simulation; parameters are the requirement for validating and evaluating the credibility and ability of the proposed cooperative mechanism in comparison to the

related works, this research parameter is highlighted in Table 2 according to the proposed mechanism and algorithms requirements.

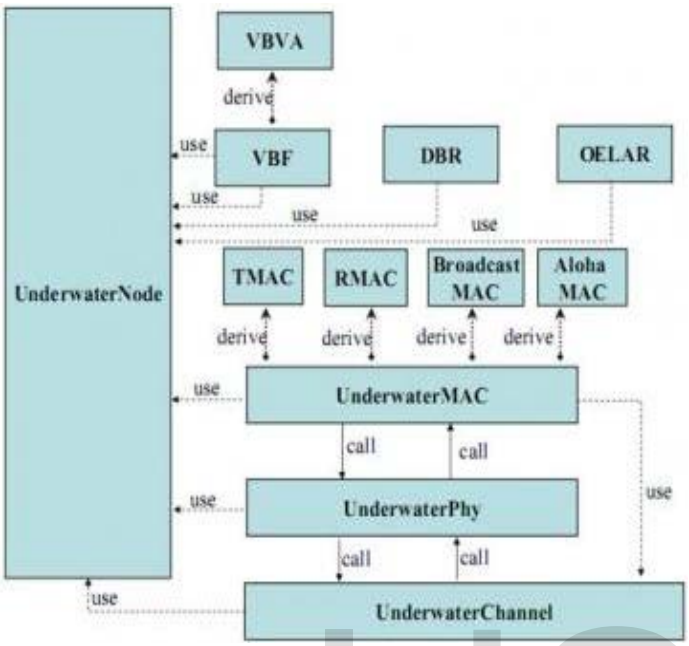


Figure 10: Aqua- Sim Architecture

Table 2: Simulation Parameter

S/N	Parameters	Values
1	Number of nodes	50, 75, 100
2	Number of Malicious nodes	0-50
3	Topology area	1000m X 1000m
4	Transmission ranges	120m
5	Maximum Transmission power	2 watts
6	Depth	100m
7	Mobility Model	Random waypoint
8	Maximum number of retransmission	3
9	Maximum motivation	2
10	Simulation time	1000 secs
11	Routing protocol	VBF hop-by-hop
12	MAC protocol	Underwater MAC/Broadcast MAC
13	Channel	Underwater Channel
14	Propagation	Underwater propagation
15	Physical	Underwater Phy
16	Antenna	OminAntenna

4 RESULTS ANALYSIS AND DISCUSSION

Results Analysis comparison and discussion

The Proposed Cooperative Mechanism (Proposed CM) has been implemented in UASNs simulator Aqua-Sim, and the experiment has achieved significant objectives by a mechanism of trust and motivating the misbehaving nodes to choose the best strategy that results in cooperation. Deployment of 100 nodes was randomly done in an area of 1000m x1000m using a random waypoint mobility with the range of 120m. The nodes find the available path for connection to the neighbor node using VBF hop-by-hop routing protocols. The proposed cooperative mechanism evaluated the strategy of regular nodes and the misbehaving node which are mixed, pure and PBE strategies. Performance evaluation was done, and the Proposed CM has been compared with some of the current works SRPDBG and TSDBG based on packet delivery ratio (PDR), nodes utilities, propagation delay, transmission overhead, and transmission latency. This experiment has been evaluated with 0-50 malicious nodes which are trying to hinder the network performance but the proposed CM is robust in evaluating the trust of the nodes and motivate the misbehaving nodes. A belief updating system was used and incorporated into PBE strategy for updating the beliefs of the nodes and resulted in reducing the utilities of misbehaving nodes and motivating them to increase the utilities of regular nodes. The network size was varied from 50-100, and a study of simulation results was done. Due to the analysis of the current works it has been found that SRPDBG and TSDBG only monitors the activities of the malicious node in the routing vector, but now with proposed CM a motivation is provided to the misbehaving nodes by enabling them to compete with regular nodes in a cooperative manner to enhanced and provides reliable packet delivery.

4.1 Propagation Delay

Propagation delay for SRPDBG, TSDBG, and Proposed CM has been measured in the simulation which is the amount of time required in executing the codes for UASNs nodes. The result shown in Figure 11 below reveals that in all the approaches the propagation delay depends on the code size (Algorithm) that means the higher the delay, the more the code size (delay increase with an increase in the code size). Moreover, also the figure shows that the proposed CM achieved less delay compared with current works this was because the analysis for identifying misbehaving node behavior was done among two nodes sender and receiver and misbehaving behavior above the motivation threshold will be reported to the all neighbor nodes.

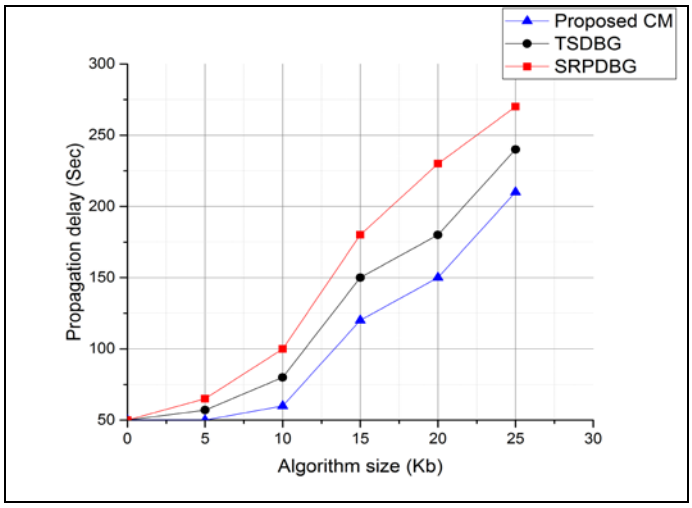


Figure 11: Propagation delay against Algorithm size

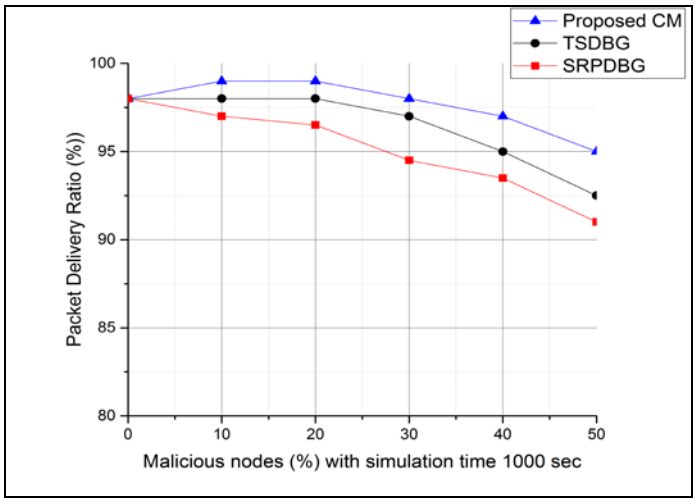


Figure 12: Packet Delivery Ratio against malicious nodes

4.2 Packet Delivery Ratio (PDR)

The impact of the malicious node was analyzed and calculate PDR, a threshold value has been set up and used by regular nodes to evaluate the trust of the neighbor nodes, and such a threshold has not been defined so that it will not violate the rationality of the node. Regular nodes choose a node among the available neighbor nodes randomly to send the packet. By default the number of malicious nodes is considered as 50 and the repetition of the simulation times is 1000 secs, it is assumed that the trust value ranges from (0-3) and two (2) is the default trust value, whenever the trust value is lower than the threshold the (default value) such a node will drop the packet and forward the packet otherwise. The dynamic threshold of the regular nodes is used to evaluate the trust of the opponent node type and motivate the misbehaving nodes only when the trust value is below the threshold. The current works does not provide effective mechanism for encouraging the nodes to cooperate in packet forwarding, Figure 12 show that the proposed CM maintained higher PDR of about 98% than the current works even when 40% of the nodes are malicious and this is due the lack of encouragement mechanism of the current works that will motivate the nodes to cooperate and also increase in the number of malicious nodes affect the detection of misbehaving node, but the proposed CM detect and encourage the misbehaving nodes to participate in packet forwarding even with dynamic change in the network topology.

4.3 Transmission overhead

Transmission overhead of the proposed CM is less than that of the two current (existing) works, and this is because in the proposed CM the malicious nodes that caused transmission overhead by dropping the packet are motivated to participate in routing unlike the two of the current works. The transmission overhead was calculated with different stages and different number of malicious nodes in which Figure 13 shows that the proposed CM has less transmission overhead of about 62% even when 50% of the nodes are malicious. In the current works the trust value calculation was based on end-to-end which caused more transmission overhead while in the proposed CM it is hop-by-hop among sender to receiver and applied motivation to the nodes involved in misbehaving activities to forward the packet to the target (receiver).

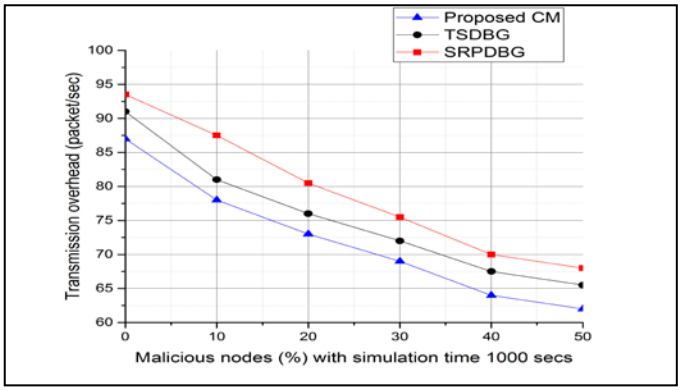


Figure 13 Transmission overhead against malicious nodes

4.4 Transmission Latency

The Latency of the proposed CM and the two of the current works SRPDBG and TSDBG was measured which is the

amount of time consumed to find the efficient route and route the packet from sender to the target node, Figure 14 illustrated that the proposed CM has 18ms latency, TSDBG is 25ms and SRPDBG is 29ms which shows that the proposed CM obtained better performance than the two current works. The latency was evaluated in different number of malicious node, and it indicates that increase in number of malicious nodes increase the transmission latency and decrease in the number of malicious nodes decrease the transmission latency. The proposed CM made use of PBE strategy to find the type of node being it regular or malicious nodes and applied a motivation to the malicious node to enable such nodes forward the packet to the target node, the regular node has less overhead and usually forward the packet to their neighbors.

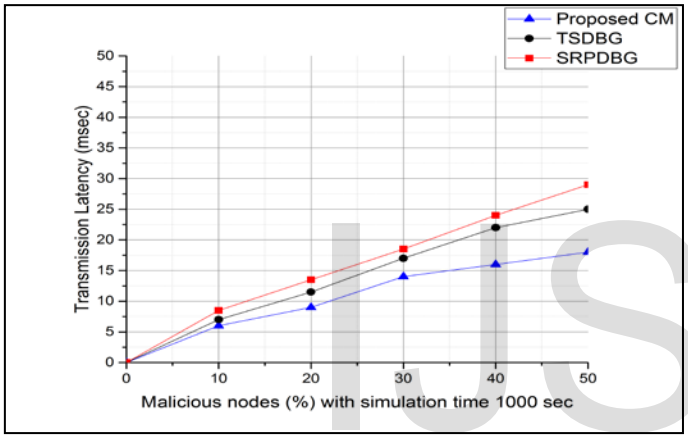


Figure 14: Transmission latency against malicious node

5. CONCLUSION, OPEN ISSUES AND RESEARCH DIRECTION

In this work, we considered the cooperation issues in UASNs which has been a challenge in many Ad Hoc Networks not only in UASNs that would degrade the performance of the network and this problem is mainly attributed by the present of misbehaving nodes in the routing vector (source-destination path) and high mobility of sensor nodes in UASNs. We studied various strategies used for UASNs in providing cooperative packet routing and proposed a s Novel cooperative model using game theory for reliable packet routing in UASNs. We developed algorithms for finding the most suitable strategy for a player and best response in providing cooperative routing in UASNs. However, the game tree was used to determine the probability distribution of each player type, the behavior of a player, action of a player and utilities of a player. Moreover, we incorporated Dynamic Bayesian game for trust evaluation and used belief updating methods to update the player belief about his opponent; our proposed CM used a motivation mechanism to encourage malicious nodes to participate in packet forwarding. The implementation was conducted using Aqua-Sim simulator used for simulating underwater environment, and the result of the experiment reveal that our proposed CM performs better than the related works regarding packet delivery ratio, propagation delay, transmission overhead and transmission latency as shown in table 3 below. Furthermore, the research outlines the feature issues and direction of research in UASNs. To the best of our knowledge based on our Literature search, our work is unique and different from all the related work describe in this paper. Most of the protocol designed for UASNs have some limitation in terms providing reliability for cooperative routing among nodes. This underwater cooperative routing is kind of cross layered approaches which required cooperation in all level of communication between sender and receiver and hence in future our focus is to designed and implement a suitable underwater protocol that would work in all layers of underwater communication by taking into consideration the limitation of all the existing underwater MAC and routing protocols. However, an End-to-End Authentication is also required to guarantee the security of packet routing among participating node and prevent the data in the packet form been compromised by the devious misbehaving nodes.

Table 3: Comparison of SRPDBG, TSDBG, and Proposed CM

Performance metrics	SRPDBG	TSDBG	Proposed CM
Propagation delay	88.33	78.29	70.02
Packet delivery ratio	91	92.5	95
Transmission overhead	68.75	65.36	62
Transmission latency	94.75	95.78	97.05

REFERENCES

[1] Jiang, Z. (2008). Underwater acoustic networks–issues and solutions. International journal of intelligent control and systems, 13(3), 152-161.

[2] Li, D.-d., Lin, Y., & Zhang, Y. (2018). A Track Initiation Method for the Underwater Target Tracking Environment. China Ocean Engineering, 32(2), 206-215.

[3] Manjula, R., & Manvi, S. S. (2011). Issues in underwater acoustic sensor networks. International Journal of Computer and Electrical Engineering, 3(1), 101.

[4] AGCEIMCY, I. A. E. (2001). Inventory of accidents and losses at sea involving radioactive material.

[5] Michel, J., Gilbert, T., Etkin, D. S., Urban, R., Waldron, J., & Blocksidge, C. T. (2005). An issue paper prepared for the 2005 international oil spill conference: Potentially polluting wrecks in marine waters. Paper presented at the International oil spill conference.

[6] Polmar, N., & Cavas, C. (2009). Navy's Most Wanted™: The Top 10 Book of Admirable Admirals, Sleek Submarines, and Other Naval Oddities: Potomac Books, Inc.

[7] Stewart, K., & Taubenfeld, R. the social and environ-

mental risks.

[8] Ragheb, M. (2012). Nuclear Marine Propulsion. University of Illinois at Urbana-Champaign.

[9] Han, G., Jiang, J., Sun, N., & Shu, L. (2015). Secure communication for underwater acoustic sensor networks. IEEE communications magazine, 53(8), 54-60.

[10] Akyildiz, I. F., Pompili, D., & Melodia, T. (2005). Underwater acoustic sensor networks: research challenges. Ad Hoc Networks, 3(3), 257-279. doi: 10.1016/j.adhoc.2005.01.004

[11] Anjum, S. S., Noor, R. M., & Anisi, M. H. (2015). Survey on MANET based communication scenarios for search and rescue operations. Paper presented at the IT Convergence and Security (ICITCS), 2015 5th International Conference on.

[12] Jin, X., Chen, Y., & Xu, X. (2016). The analysis of hops for multi-hop cooperation in Underwater Acoustic Sensor Networks. Paper presented at the Ocean Acoustics (COA), 2016 IEEE/OES China.

[13] Abdul-Salaam, G., Abdullah, A. H., & Anisi, M. H. (2017). Energy-efficient data reporting for navigation in position-free hybrid wireless sensor networks. IEEE Sensors Journal, 17(7), 2289-2297.

[14] Jha, V. (2012). QoS Issues In Underwater Sensor Networks. 45-51. doi: 10.5121/csit.2012.2206

[15] Pompili, D., Melodia, T., & Akyildiz, I. F. (2010). Distributed routing algorithms for underwater acoustic sensor networks. IEEE Transactions on Wireless Communications, 9(9), 2934-2944.

[16] Karatas, M., Craparo, E., & Akman, G. (2018). Bistatic sonobuoy deployment strategies for detecting stationary and mobile underwater targets. Naval Research Logistics (NRL), 65(4), 331-346.

[17] Lal, C., Petroccia, R., Conti, M., & Alves, J. (2016). Secure underwater acoustic networks: Current and future research directions. Paper presented at the Underwater Communications and Networking Conference (UComms), 2016 IEEE Third.

[18] Silva, B. M., Rodrigues, J. J., Kumar, N., & Han, G. (2015). Cooperative strategies for challenged networks and applications: A survey. IEEE Systems Journal.

[19] Liu, C.-G., Chao, C.-H., Leou, C.-W., & Li, J.-S. (2012). Iterative key distribution based on MAD neighborhood in underwater mobile sensor networks. The Computer Journal, bxs031.

[20] Zuba, M., Shi, Z., Peng, Z., Cui, J.-H., & Zhou, S. (2015). Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks. Security and Communication Networks, 8(16), 2635-2645. doi: 10.1002/sec.507

[21] Giordan, D., Hayakawa, Y., Nex, F., Remondino, F., & Tarolli, P. (2018). the use of remotely piloted aircraft systems (RPASs) for natural hazards monitoring and management. Natural Hazards and Earth System Sciences, 18(4), 1079-1096.

[22] Al-Dharrab, S., Uysal, M., & Duman, T. M. (2013). Cooperative underwater acoustic communications [Accepted from open call]. IEEE communications magazine, 51(7), 146-153.

[23] Lodeiro-Santiago, M., Santos-González, I., Caballero-Gil, C., Caballero-Gil, P., & Herrera-Priano, F. (2018). Novel Guidance CPS Based on the FatBeacon Protocol. Applied Sciences, 8(4), 647.

[24] Carbonelli, C., Chen, S.-H., & Mitra, U. (2009). Error propagation analysis for underwater cooperative multi-hop communications. Ad Hoc Networks, 7(4), 759-769. doi: 10.1016/j.adhoc.2008.03.007

[25] Anisi, M. H., Abdullah, A. H., & Razak, S. A. (2011). Efficient data aggregation in wireless sensor networks. Paper presented at the International Conference on Future Information Technology IPCSIT.

[26] Li, Z., & Shen, H. (2012). Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. IEEE transactions on mobile computing, 11(8), 1287-1303.

[27] Li, F., Yang, Y., & Wu, J. (2010). Attack and flee: game-theory-based analysis on interactions among nodes in MANETs. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 40(3), 612-622.

[28] Dini, G., & Lo Duca, A. (2012). A secure communication suite for underwater acoustic sensor networks. Sensors, 12(11), 15133-15158.

[29] Dini, G., & Lo Duca, A. (2012). A secure communication suite for underwater acoustic sensor networks. Sensors (Basel), 12(11), 15133-15158. doi: 10.3390/s121115133

[30] Kaliappan, M., & Paramasivan, B. (2015). Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game model. Computers & Electrical Engineering, 41, 301-313. doi: 10.1016/j.compeleceng.2014.11.011

[31] Xie, Y., & Zhang, Y. (2016). A secure, service priority-based incentive scheme for delay tolerant networks. Security and Communication Networks, 9(1), 5-18.

[32] Ahmed, M. R., Aseeri, M., Kaiser, M. S., Zenia, N. Z., & Chowdhury, Z. I. (2015). A novel algorithm for malicious attack detection in uwsn. Paper presented at the Electrical Engineering and Information Communication Technology (ICEEICT), 2015 International Conference on.

[33] Boudec, J. A robust reputation system for p2p and mobile ad-hoc networks. Paper presented at the Proceedings of the 2nd Workshop on the Economics of Peer-to-Peer Systems.

[34] Li, Y., Xu, H., Cao, Q., Li, Z., & Shen, S. (2015). Evolutionary Game-Based Trust Strategy Adjustment among Nodes in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 11(2), 818903. doi: 10.1155/2015/818903

[35] Rafsanjani, M. K., Aliahmadipour, L., & Javidi, M. M. (2012). A hybrid Intrusion Detection by game theory approaches in MANET. Indian Journal of Science and Technology, 5(2), 2123-2131.

[36] Dong, Y., & Liu, P. (2010). Security considerations of underwater acoustic networks. Paper presented at the Proceedings of the International Congress on Acoustics (ICA'10), Sydney, Australia.

[37] Mohammed, N., Otrok, H., Wang, L., Debbabi, M., & Bhattacharya, P. (2008). A mechanism design-based multi-leader election scheme for intrusion detection in manet. Paper presented at the Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE.

[38] Ng, S.-K., & Seah, W. K. G. (2008). Game-theoretic model for collaborative protocols in selfish, tariff-free, multi-hop wireless networks. Paper presented at the INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.

[39] Buchegg, S., & Boudec, J. (2004). A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks. Paper presented at the Proc. of the 2nd Workshop on the Economics of Peer-to-Peer Systems.

[40] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A survey of game theory as applied to network security. Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

[41] He, D., Chen, C., Chan, S., & Bu, J. (2012). SDRP: A secure and distributed reprogramming protocol for wireless sensor networks. IEEE Transactions on Industrial Electronics, 59(11), 4155-4163.

[42] Lee, J., & Oh, J. C. (2014). Convergence of True Cooperations in Bayesian Reputation Game. Paper presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on.

[43] Paramasivan, B., Prakash, M. J. V., & Kaliappan, M. (2015). Development of a secure routing protocol using game theory model in mobile ad hoc networks. Journal of Communications and Networks, 17(1), 75-83.

[44] Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., & Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE Access, 5, 15619-15629.

[45] Nurmi, P. (2004). Modelling routing in wireless ad hoc networks with dynamic Bayesian games. Paper presented at the Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on.

[46] Ayday, E., & Fekri, F. (2010). A protocol for data availability in Mobile Ad-Hoc Networks in the presence of insider attacks. Ad Hoc Networks, 8(2), 181-192. doi: 10.1016/j.adhoc.2009.07.001

[47] Jiang, J., Han, G., Shu, L., Chan, S., & Wang, K. (2015). A Trust Model based on Cloud Theory in Underwater Acoustic Sensor Networks. IEEE Transactions on Industrial Informatics.

[48] Anisi, M. H., Abdullah, A. H., & Razak, S. A. (2012). Efficient data gathering in mobile wireless sensor networks. Life Science Journal, 9(4), 2152-2157.

[49] Jin, X., Pissinou, N., Pumpichet, S., Kamhoua, C. A., & Kwiat, K. (2013). Modeling cooperative, selfish and malicious behaviors for trajectory privacy preservation using bayesian game theory. Paper presented at the Local Computer Networks (LCN), 2013 IEEE 38th Conference on.

[50] Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., & Hubaux, J.-P. (2013). Game theory meets network security and privacy. ACM Computing Surveys, 45(3), 1-39. doi: 10.1145/2480741.2480742

[51] Musacchio, J., & Walrand, J. (2006). WiFi access point pricing as a dynamic game. IEEE/ACM Transactions on Networking (TON), 14(2), 289-301.