

## Trust model genetic node recovery based on cloud theory for underwater acoustic sensor network

Buddesab, Thriveni J, Venugopal K R

Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,  
Bangalore University, India

---

### Article Info

#### Article history:

Received Jan 11, 2019

Revised Apr 8, 2019

Accepted Apr 16, 2019

---

#### Keywords:

Cloud Theory Model

Data security

TWSN

UASN

Wireless Sensor Network

---

### ABSTRACT

Underwater Acoustic Sensor Networks [UASNs] are becoming a very growing research topic in the field of WSNs. UASNs are harmful by many attacks such as Jamming attacks at the physical layer, Collision attacks at the data link layer and Dos attacks at the network layer. UASNs has a unique characteristic such as unreliable communication, mobility, and computation of underwater sensor network. Because of this the traditional security mechanism, e.g. cryptographic, encryption, authorization and authentications are not suitable for UASNs. Many trust mechanisms of TWSNs [Terrestrial Wireless Sensor Networks] had proposed to UASNs and failed to provide security for UASNs environment, due to dynamic network structure and weak link connection between sensors. In this paper, a novel Trust Model Genetic Algorithm based on Cloud Theory [TMC] for UASNs has been proposed. The TMC-GA suggested a genetic node recovery algorithm to improve the TMC network in terms of better network lifetime, residual energy and total energy consumption. Also ensures that sensor nodes are participating in the rerouting in the routing discovery and performs well in terms of successful packet delivery. Simulation result provides that the proposed TMC-Genetic node recovery algorithm outperforms compared to other related works in terms of the number of hops, end-to-end delay, total energy consumption, residual energy, routing overhead and network lifetime.

*Copyright © 2019 Institute of Advanced Engineering and Science.  
All rights reserved.*

---

### Corresponding Author:

Buddesab,

Department of Computer Science and Engineering,

University Visvesvaraya College of Engineering,

Bangalore, Bangalore University, 560001- India.

Email: tonnur21@gmail.com

---

## 1. INTRODUCTION

UASNs are specially designed to operate and monitor under water such as the ocean, lake, etc and communication frequency of operation is between 10 Hz and 1 MHz UASNs have unique characteristics such as acoustic channel communication, weak link connection, dynamic network, and mobility. Due to this providing security to UASNs is not as easy as TWSNs. In UASN, network structure operates first under water and sends the information to the local station and then forward to the base station [1]. Underwater acoustic sensor network (UASN) deals with the propagation of underwater sound and interaction of mechanical waves that generate noise with water. A UASN has many small sensor nodes which are placed underwater that relatively cooperate in gathering information about the environment and satisfying the challenging requirements. Acoustic Wireless Sensor Network consists of sensors and vehicles which form an autonomous network for collaborative monitoring tasks. The applications of UASN are Monitoring heavy instruments, controlling weather pollution, Climate Reporting, natural disturbances causes, prediction, Marine Life Study, Ocean surveillance and disaster prevention [2].

Wireless sensor networks are sensor nodes which are spatially distributed over a network that collaborate with each other to collect information from one node to another node. WSNs have a quality to sense physical condition, e.g. weather temperature, pressure, and sound. WSNs co-operatively collect detected information to the local station and pass to the central station. WSNs architecture involves the OSI model which includes the application layer, transport layer, network layer, data link layer, and physical layer. WSNs are widely used in the many areas such as civilian, industry, and army, and some of the WSNs applications are Fire Detection, Industrial Process Monitoring, Monitoring Traffic and Health care monitoring, etc [3].

Cloud theory model is a cloud technology firm specializing based on cloud computing concepts. Cloud theory concept run on the internet as a base platform to provide service to a user from servers. Cloud model maintains central remote stations to save data and application and manage the data to the user. Cloud model provide services to a user on demand on the internet with the secure network access for a share of configurable and computing resources such as servers, networks, data storage, applications, and application services. Cloud Model provide lower operating cost and maintain ace cost to providers [4].

Terrestrial Wireless Sensor Networks[TWSNs] are specially designed to provide services based on land. TWSNs include 'air' has the primary communication channel to supply connected information from one node to another. TWSNs mainly consist of sending and receiving devices to send and receive information and carries data or voice information via electromagnetic radio waves. The typical traditional security mechanisms have been suggested to provide security to Terrestrial Wireless Sensor Network such as Cryptography, Authentication, Confidentiality, and Availability.

A Trust Management System (TMS) has been recently suggested to provide energy efficient and handle attacks in many layers and improved node cooperation in successful packet delivery, localization of node. In the Trust Management Scheme for sensor networks security (TMS), the forwarding node is chooses based on the behavior of neighbor nodes, and the direct trust computation is performed. The TMS maintains a database at each node level to preserve the trust. The routing mechanism can perform back and forth propagation because of which there is massive amount of energy loss and also since the node delivers the packet the direct trust will also get incremented which is incorrect.

The TMS approach has the following disadvantages,

- a. The trust computation depends on the Expected Transmission Count (ETC) which is the direct trust for the nodes.
- b. There is a lot of energy wastage due to back and forth propagation involved in the routing path.
- c. The trust mechanism does not take into consideration the bit error rate on the physical medium which is a significant impact in the underwater environment.
- d. The TMS algorithm trust measure is not good because abnormal packet forwarding is caused by not only malicious attacks but also unreliable acoustic channel and uncertain underwater environment, e.g., ocean currents.

Nodes in the wireless sensor network are prone to failure due to energy depletion, hardware failure, and communication link errors, etc. "Fault node recovery algorithm" detects a fault node when some sensor nodes shutdown due to low battery energy. The genetic algorithm is used to recover the depleted node in the network. The node depletion may be due to no available power, or it may reach the threshold level. The main aim to identify the dead nodes and then find few nodes to be replaced among them so that the cost of maintenance is reduced and overall network lifetime is periodically increased. During TMC trust model evolution, the following two concerns have been taken into consideration to provide a better QoS to network in terms of the network lifetime and residual energy

- a. The network lifetime has taken into account to improve the overall lifetime of the system by providing efficient energy power to the network nodes so that they can participate in the routing and it decreases the dead nodes in the network.
- b. The residual energy of the network will be maintained well in the TMC model by proving sufficient energy to nodes which are suffering from insufficient energy power to participate in the routing and data communication.

We propose a TMC genetic node recovery model to improve TMC model in terms of network lifetime, the residual energy of network, QoS and also reduces dead nodes as well. The contributions as follows. The proposed model first identifies the faulty which are below the defined threshold level. In the network after some iteration and data communication between source and destination apply the genetic process-selection, crossover, mutation to the nodes. Then it recovers the faulty nodes with the required energy whose values are one from the genetic process. Hence the recovered nodes can be used for rerouting in the network and also can participate in the data packet transmission from source to destination thus improve network residual energy and network lifetime.

The remainder of this paper is organized as follows: In Section 2, we review the related work. In Section 3, the system model and design are presented. Section 4 provides a detailed description of the proposed TMC-GA trust model. Section 5 the proposed algorithms. Section 6 presents the simulation results and related performance analysis. Finally, conclusions are drawn in Section 7.

## 2. RELATED WORK

Ganeriwal et al. [5] have analyzed Reputation-based Framework for implementing some trustworthy sensor nodes at runtime based on the neighbor node behavior. Yao et al. [6] have investigated the sensor network security with trust management methods. "PLUS: Parameterized and Localized trUst management Scheme" for protection of sensor network to provide user trusted environment has been proposed to guarantee the network security issues efficiently. Feng et al. [7] have integrated the approach of nodes behavior strategies and modified evidence theory. Various trust factors and coefficient are considered to get trust values of direct and indirect trust. NBBTE used Fuzzy logic methods are used to fetch the node trust levels and D-S evidence theory based on the levels of trustworthiness

Ren et al. [8] have handled the information related to trust with a secure and efficient way for Unattended Wireless Sensor Network (UWSNs) and provide a trust data storage with scalable, more efficient and trust generation. Boukerche et al. [9] have introduced a trust and reputation management schemes with the mobile agents running on each node. Agent-based Trust and Reputation Management scheme (ATRM) system calculates trust and reputation using the mobile agent. Shaikh et al. [10] have evaluated the group of sensor nodes trust that provides methods to identify the attacker's malicious sensor nodes along with small prevention mechanism degree.

Han et al. [11] have proposed Attack-Resistant Trust model based on Multidimensional trust Metrics (ARTMM) that ensures a more efficient and reliable UASNs network. Domingo et al. [12] have introduced Ray-theory-based multipath Rayleigh underwater model for efficient data communication in Underwater Wireless Communication Networks (UWCN). Sound propagation calculation, transmission losses between transceivers and investigated bit error rate effects has been considered to implement effective communication. Lim et al. [13] have introduced a systematic method for sensor network called "Provenance based Trustworthiness Assessment" adopted which generates a) data item trust score values b) evaluation of network node trust score value.

Jiang et al. [14] have described providing trust in the WSNs and Efficient Distributed Trust Model (EDTM) evaluates the trustworthiness of sensor nodes more precisely. Subjective logic probability density function considered assessing direct communication trust, data packet trust, link communication trust, network or node energy trust. Jiang et al. [15] have provided the safety of Underwater Mobile Sensor Network. This research includes the neighbor nodes monitor loss and error of data packets, sensor node energy consumption, Trust level are considered to evaluate the trust evidence and direct trust, indirect Trust, historical trust, recommendation trust, data trust also been studied for trust calculation. Juelong et al. [16] have introduced LARP used to minimize the network delay in terms of transmission, ensuring less energy consumption in the network and provide better network communication quality. Chen et al. [17] have proposed to identify attacked malicious sensor nodes in various events. It detects malicious sensor nodes and notifies the network along with different event trust rating.

Qu et al. [18] have introduced the improvement of trust mechanisms with the defending methods. "Watchdog and Trust mechanism" has been proposed to analyze the security of network from the inside and "Defending methods" used to analyze trust mechanism and watchdog in terms of network lifetime. Han et al. [19] have introduced to ensure location security of the network. This research provides node location in terms of good accuracy and better reliability from the defined trust model which minimize the unknown nodes localization error and enhances localization accuracy. Kim et al. [20] have proposed to analyze proper trust models with the right communicating an approach to get the reliable path from source node to destination node. The following methods are considered to implement trust; they are the degree of each node is calculated to decide whether to communicate or not and trust level of the sensor node is estimated to communicate within the transmission range.

Batish et al. [21] have proposed "Efficient Weighted Trust Evaluation System for Wireless Sensor Networks (WTES-WSN)" to significantly increase the network efficiency and minimize the trust evaluation cost. Sarkodee et al. [22] have described that reputation and trust are divided into various classes or categories. Referencing method is used in providing researchers with a tool that makes it easier to reference the features on reputation and trust in a much easier way than if referencing has to be directed to several uncoordinated resources.

Solanki et al. [23] have reviewed the existing data security architecture and key management system in WSN. The proposed security technique offers a fruitful solution to secure data transmission among the low battery life and tiny devices, used in WSN due to its low time and space complexities.

### 3. SYSTEM MODEL AND DESIGN

#### 3.1. System model

UASNs Consists of a multi-hop homogeneous network that is initially all the underwater sensor nodes have an equal amount of initial energy level, the same capability of communication, computation, and storage. In the UASN, there are  $n$  tiny sensor nodes, denoted by  $s_i \in S$ , where  $S = \{s_i\}_{i=1}^n$ . Each sensor node  $s_i$  is randomly deployed at the position  $p_i$  with the communication range  $r$ . The two neighbor nodes can directly communicate with each other only when the distance  $d(p_i, p_j)$  between two neighbor nodes  $s_i$  and  $s_j$  satisfies  $d(p_i, p_j) \leq r$ .

In the UASNs network considering 3 kinds of node, they are trustor, trustee and recommended. When a sensor node A wants to get the trust of another sensor node B, the evaluated node B is named as a trustee node. Based on communication behaviors between neighbor nodes, a trustor can judge whether a trustee is trustworthy or not. If there are direct communications between trustor and trustee, direct trust is calculated. Indirect trust is computed based on other sensor nodes recommendations. The sensor node which is providing recommendations is named as a recommender.

#### 3.2. System design

During Software development, System Design is considered a critical and essential phase of the development phase. The design part of the growth will have more logical data and theoretical ideas to fulfill the requirements of functional and non-functional requirements of development. Small systems are easy to design with minimum requirements whereas large system required to integrate with subsystems services to satisfy requirements. System architecture will be the output of system design in software development.

### 4. TMC-GA TRUST MODEL

#### 4.1. Objectives

In the TMC method, the forwarding node before being selected undergoes a lot of test/parameters measure which is responsible for picking the forwarding node. It takes into consideration both direct trusts as well as indirect trust in the trust computation. During the trust computation packet loss, energy consumption and the packet error rate is taken which improves the accuracy. The routing process in the proposed method maintains a field known as 'Node in Route' which supports the information of all the traversed nodes during the routing process.

#### 4.2. TMC-genetic node recovery methodology

The structure of TMC-Genetic Node recovery is shown in Figure 1 TMC-GA trust computation methodology consists of three parts.

- 1 Trust evidence generation.
- 2 Direct trust calculation.
- 3 Recommendation and indirect trust calculation.
- 4 Genetic Node recovery Algorithm.

#### 4.3. Trust evidence generation

In current trust models, packet loss is widely used as an important trust metric. However, getting statistics like the number of replied ACK packets as trust evidence is not reliable in an underwater environment. A novel trust model named TMC, in which packet loss is analyzed layer by layer to avoid the influence from an unreliable acoustic channel and dynamic network structure.

##### 4.3.1. Packet loss based trust evidence

The packet loss is observed and evaluated between OSI layers from the physical layer to the transport layer. The acoustic channel is characterized by high bit error and temporary loss of connectivity. High bit error easily causes serious data packet loss, which can be calculated as follows. First, the path loss of the acoustic signal is obtained as:

$$A(l, f) = A_0 l^k a(f)^l \quad (1)$$

where  $l$  is the transmission distance,  $f$  is the frequency of the acoustic signal,  $a(f)$  is the absorption coefficient and  $A_0$  is a normalization constant,  $k$  is the energy propagation coefficient and in general, for the spherical spreading,  $k = 2$ .

Based on the path loss  $A(l, f)$  and the power spectral density  $N(f)$ , the signal-to-noise ratio (SNR) of the acoustic channel can be calculated by

$$SNR(l, f) = \frac{P/A(l, f)}{N(f) \Delta f} \tag{2}$$

The total power spectral density depends on the four kinds of noises. i.e ocean background noise(turbulence), shipping, waves and thermal noise [12].

1. Ocean background noise (turbulence noise)  $10 \log N_t(f) = 17 - 30 \log f$
2. Shipping noise  $10 \log N_s(f) = 40 + 20(s - 0.5) + 26 \log f - 60 \log(f + 0.03)$
3. Waves  $10 \log N_w(f) = 50 + 7.5w^{1/2} + 20 \log f - 40 \log(f + 0.4)$
4. Thermal noise  $10 \log N_{th}(f) = -15 + 20 \log f$   
Where  $N_{th}(f)$  = thermal noise

Binary Phase Shift Keying (BPSK) modulation is used to transmit the data as the physical layer medium. Hence the packet loss can be computed using,

$$P_{loss-phy} = (1 - \frac{1}{2} \operatorname{erfc} \sqrt{SNR})^b \tag{3}$$

where  $P_{loss-phy}$  = path loss for physical layer,  $b$  = number of bits pattern

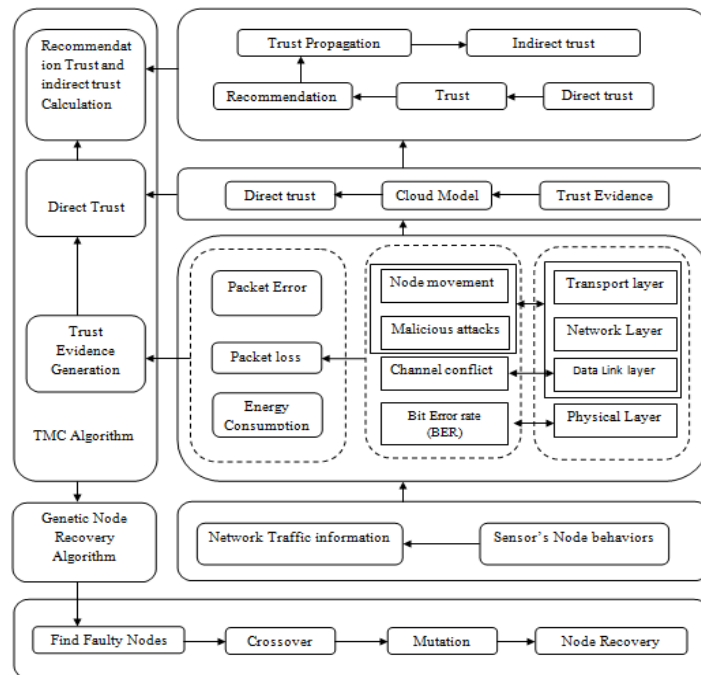


Figure 1. TMC -GA trust computation methodology

#### 4.3.2. MAC layer packet loss

The MAC Layer packet loss can be obtained as below (4)

$$P_{loss-max} = \frac{N_{send}}{N_{ack}} \tag{4}$$

where  $N_{ack}$ =Number of ACK packets,  $N_{send}$ =Number of packets send

$P_{loss-mac}$ =Loss of MAC packets

#### 4.3.3. Transport layer packet loss

The Transport layer packet loss is treated as zero because before the node sends a packet to the node it dynamically determines neighbors each time.

$$P_{loss-tran}=0 \quad (5)$$

#### 4.3.4. Network layer

In the network historical trace is obtained which is responsible for finding or predicting the packet loss with the compromised nodes using a linear model over a period for a time series data using FARIMA method [24]. The equation gives the total packet loss

$$P_{loss} = P_{loss-mac} + P_{loss-pre} + P_{loss-phy} \quad (6)$$

#### 4.4. Trust evidence–packet error

The Trust Evidence depends upon the error rate of the packet. The packet error rate is computed by checking the data item and number of bits which were lost over a period [13].

$$P_{loss} = 1 - 2 \left( 0.5 - \int_{\mu_x}^{v_d} f(x) dx \right) \quad (7)$$

Where  $v_d$  is the computed data item numerical.  $\mu_x$  is the sensed data items mean value.  $f(x)$  is the data items probability density function.

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x - \mu_x)^2}{2\sigma^2}} \quad (8)$$

#### 4.5. Trust evidence–energy consumption

The energy consumptions is given by the following (9),

$$P_{energy} = 1 - \frac{E_{res}}{E_o} \quad (9)$$

where  $E_{res}$ =residual energy of node,  $E_o$ =initial energy

The parameter total energy consumption is given as follows

$$TE_c = \sum_{i=1}^l E_i \quad (10)$$

where  $l$ =number of links,  $E_i$ =Energy consumed by the  $i^{th}$  link

The energy consumed by the  $i^{th}$  link given by, where Energy required for data transmission is more than the energy needed for data generation.

$$E_c = 2E_{tx} + E_{amp} d^\gamma \quad (11)$$

where  $E_{tx}$ =energy required for data transmission,  $E_{amp}$ =energy required for data generation  
 $d$ =distance between two intermediate node,  $\gamma$ =environment factor  $0.1 \leq \gamma \leq 1$

#### 4.6. Trust recommendation computation

The trust recommendations are computed based on the following measure. If  $m$  they represent the number of neighbors, then the resulting trusts are calculated [14].

$$E_x = \frac{1}{M} \prod_{i=1}^m E_{xi}$$

$$E_n = \min\left\{\frac{1}{m} \sum_{i=1}^m E_{ni}, 1\right\} \quad (12)$$

$$E_e = \min\left\{\frac{1}{m} \sum_{i=1}^m E_{ei}, 1\right\}$$

#### 4.7. Direct trust computation

The value of direct communication trust is computed using below equations [25].

$$\begin{aligned}
 Exi &= xi^- \\
 xi^- &= \frac{1}{n} \sum_{i=1}^n xi \\
 E_{ni} &= \frac{\sqrt{\pi}}{2} \frac{1}{n} |Exi - xi| \\
 E_{ei} &= \text{root} (S^2 - E_{ni}^2)
 \end{aligned}
 \tag{13}$$

Where  $n$  = number of attribute,  $x_i$  = attribute value

The above values are computed based on packet loss, packet error, and energy consumed.

### 5. ALGORITHMS

#### 5.1. TMS algorithm

Algorithm 1: TMS Routing Algorithm

Step 1 : TMS takes inputs as Source Node, Destination Node, and Transmission Range.

Step 2 : First, the Source Node will be responsible for collecting neighbor node list which is within communication range provided.

Step 3 : Stop the process if the Source node- neighbor node list contains the destination node.

Step 4 : If the neighbor node list does not include the destination node then calculate the Direct trust of each of the neighbor nodes based on  $E_{tx}$  value.

$$TE_{tx} = \sum_{i=0}^N Etxi / N$$

$$E_{tx} = N_{ACK} / N_{gen}$$

Step 5 : Pick a node which has the highest trust value and repeats the process until the destination is reached.

#### 5.2. TMC-routing algorithm

Algorithm 2: TMC Routing Algorithm

Step 1 : TMC takes input as Source Node, Destination Node, and Communication. Transmission Range.

Step 2 : First, the Source Node will be responsible for collecting neighbor node list which is within in communication range provided.

Step 3 : Stop the process if the Source node-neighbor node list contains the destination node.

Step 4 : If the neighbor node list does not include the destination node then find neighbour. Nodes using the NIR list.

Step 5 : For the new neighbors generate trust evidence.

Step 6 : For the new neighbors compute direct trust.

Step 7 : For the new neighbors compute trust recommendations using indirect trust measure.

Step 8 : Pick up a node which has the highest trust measure.

Step 9 : Repeat process until the destination is reached.

#### 5.3. TMC-genetic node recovery algorithm

Nodes in the wireless sensor network are prone to failure due to energy depletion, hardware failure, and communication link errors, etc. "Fault node recovery algorithm" detects a fault node when some sensor nodes shutdown due to low battery energy. The genetic algorithm is used to recover the depleted node in the network. The node depletion may be due to no available power or it may reach the threshold level.

Algorithm 3: TMC Genetic Node Recovery Algorithm

Step 1 : Source Node, Destination Node, and Transmission Range acts as an input.

Step 2 : The Source Node will find the set of nodes within transmission range known as neighbor nodes.

Step 3 : If the neighbor nodes have the destination node then stop the process.

Step 4 : If the neighbor nodes do not have the destination node then compute the neighbor Nodes using the NIR list.

Step 5 : For the new neighbors generate trust evidence

Step 6 : Genetic process is triggered for every T iterations to recover the faulty nodes

Step 7 : Find the count of number of faulty nodes in the network. Faulty nodes are set of Nodes which do not have sufficient amount of energy required for transmission.

Step 8 : If no faulty nodes in the network, the genetic algorithm stops.

- Step 9 : If a faulty node exists then generate a set known as chromosomes are generated which depends on the number of faulty nodes. The chromosome size is equal to the number of faulty nodes.
- Step 10 : Consider a set of four chromosomes {CZ1,CZ2,CZ3,CZ4}.
- Step 11 : Suppose the set of nodes {5,9,15,20,23,35,40,45,55,60}. The size of faulty nodes is Ten then there are four chromosomes which are randomly generated with the values of zero and ones as given by the following values.  
 CZ1={0,0,1,0,1,1,0,1,1,0}  
 CZ2={1,1,0,0,0,1,0,1,0,1}  
 CZ3={0,0,1,0,1,1,0,1,0,1}  
 CZ4={1,1,0,0,0,1,0,1,1,0}
- Step 12 : Select best two chromosomes.
- Step 13 : Then apply crossover as shown in Figure 2 crossover function and mutation process as shown in Figure 3 Mutation function.
- Step 14 : Replace nodes whose value is 1.
- Step 15 : Genetic algorithm stops and TMC routing algorithm continues to execute for rest of iteration

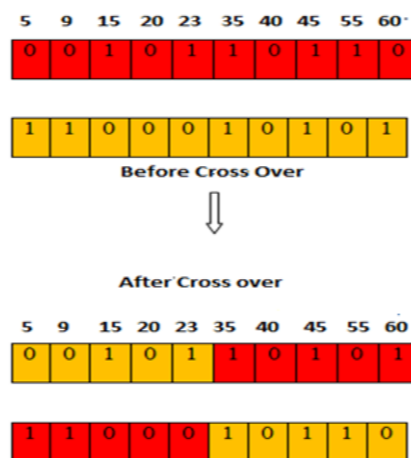


Figure 2. Crossover function

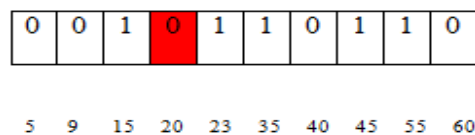


Figure 3. Mutation function

## 6. PERFORMANCE EVALUATION

### 6.1. QoS parameters used to evaluate of the TMC, TMS, and TMC-GA algorithms

Simulation of TMC is performed against TMS and evaluated performance with the following parameters,

1. End to End to Delay (Round Trip Time)
2. Number of Hops
3. Total Energy Consumption
4. Residual Energy
5. Routing Overhead
6. Network Lifetime

Simulation is performing with multiple sources and destination nodes in the network. The number of nodes in the system set to 30, initial battery energy set to 1000MJ, and Transmission range of sensor nodes set to 40m. Multiple sources and the destination is defined in the simulation therefore data transmission takes place between each source and destination.



**6.2. Simulation setup**

We conduct a simulation in Matlab to evaluate the performance of TMC-GA. The sensor network is set up where the environmental condition needs to be monitored. The deployed sensor gathers the data, and then this data is sent to the Service Providers. The CSPs then organize the information according to the specific fields. The users can approach the stored secure data in the cloud over the internet. The hard disk 40GB and RAM is set to 35 GB. The Operating System is Windows 8.1/XP is used with the JAVA/J2EE coding language. The integrated development environment is Net Beans 6.9.1 with MYSQL database. The visual interface is set to command line prompt.

**6.3. Performance Analysis**

**6.3.1. End to end to delay (round trip time)**

End to End delay defined as time taken by the route request (RREQ) packets to travel from the source to destination node and for a route reply (RREPLY) to come back from the destination to source node. End to end delay measures one round trip time taken by source and destination to traverse the network within the transmission range to deliver data packets in the wireless sensor network. Here End to End to delay is calculated by a timer.

$$E2Edelay = tstart - tstop$$

End to end delay simulation is performed against three defined algorithms. In the simulation comparison results of TMS, TMC, and TMC-genetic node recovery algorithm, TMC, and TMC-Genetic node recovery algorithm has taken less time compared to TMS because in TMS routing algorithm routing may undergo back and forth propagation to fetch next node in the network. TMS routing algorithm may visit more than one node in the routing process whereas TMC and TMC-Genetic node recovery algorithm does not visit nodes twice in the network. TMC algorithm minimizes end to end delay to guarantee the quality communication channel from source to destination and more energy efficient. Figure 4 End-to-End delay performance shows that TMC-Genetic node recovery algorithm is performed better than the TMS and TMC algorithm in terms of milliseconds.

**6.3.2. Number of hops**

The number of hops is defined as the number of intermediate links or nodes between the source node and destination node per route. The number of hops simulation comparison shown in Figure 5. TMC and TMC-Genetic node recovery algorithm have taken fewer hops compared to TMS routing algorithm because in TMS routing algorithm some routing may undergo back forth propagation to fetch the next node in the network. Therefore, TMS routing algorithm may visit an already visited node in the routing process whereas TMC and TMC-Genetic node recovery algorithm does not visit nodes twice in the network. Hence in TMS routing algorithm a route may have repeated nodes in the network, and also TMS algorithm may cross the total number of available nodes in the system.

TMC algorithm number of hops falls within total number available nodes in the network, and this will guarantee that quality communication channel from source to destination, increases the number of alive nodes in the network thus increases network lifetime, increase residual energy of nodes and therefore energy efficient than the TMS algorithm.

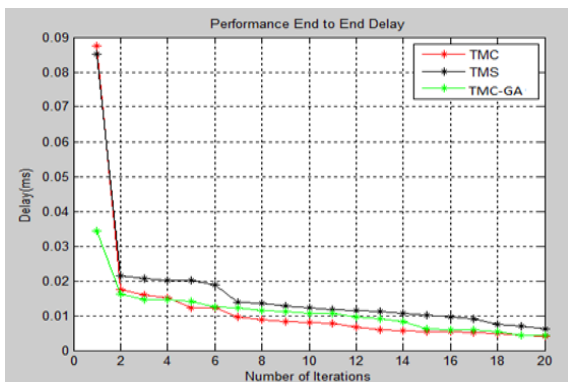


Figure 4. End-to-End delay performance of TMC, TMS, and TMC-GA

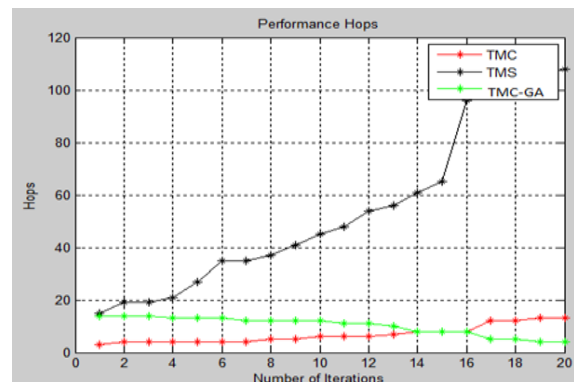


Figure 5. Number of Hops Performance of TMC, TMS, and TMC-GA

### 6.3.3. Total energy consumption

Energy consumption is defined as spending energy by the node in terms of node generation, data transmission, and route discovery. The total energy consumption defines that total wasted energy for delivering the packets from the source node to the destination node in the route. Overall energy consumption simulation comparison is shown in Figure 6. TMC and TMC-Genetic node recovery algorithm have consumed less energy compared to TMS routing algorithm because in TMS routing algorithm some routing may undergo back and forth propagation to fetch next forward node in the network. Hence in TMS routing algorithm a route may have repeated nodes in system whereas TMC and TMC-Genetic node recovery algorithm does not visit nodes twice in the network. The number of hops increases in the network which leads to the total energy consumption increases. TMS algorithm is less energy efficient compared to TMC and TMC-Genetic node recovery algorithm. Figure 6 shows the Performance energy consumed shows that TMS consumed higher than the TMC algorithm and TMC-Genetic node recovery algorithm.

### 6.3.4. Residual energy

Residual energy of all the nodes in the network defines that total available energy of all nodes in the network over a periodic time. This is the total remaining energy in the network. Some routing network will have Residual Energy Limits (REL) where some routing network will not have a REL concept. TMS algorithm will not have REL concept whereas the TMC algorithm has REL. REL is calculated by Energy consumption by nodes.

Residual energy simulation comparison is shown in Figure 7. TMC-Genetic node recovery algorithm has more residual energy compared to TMC and TMS routing algorithm because in TMS routing algorithm has back and forth propagation. The number of hops increases in the network which leads to the total energy consumption increases. TMS algorithm is less energy efficient compared to TMC and TMC-Genetic node recovery algorithm. TMC-Genetic node recovery algorithm recovers the nodes to make the network more energy efficient, increases the network life and increases the number of alive nodes in the system to make available for data communication from source to destination. Figure 7 shows the Performance Residual Energy shows that TMC-Genetic node recovery algorithm has high residual energy than the TMS and TMC routing algorithm.

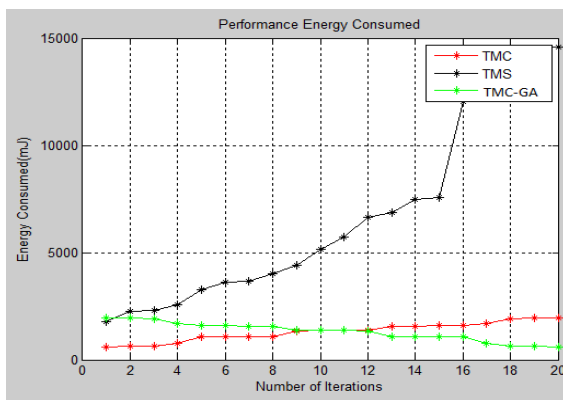


Figure 6. Performance energy consumed of TMC, TMS, and TMC-GA

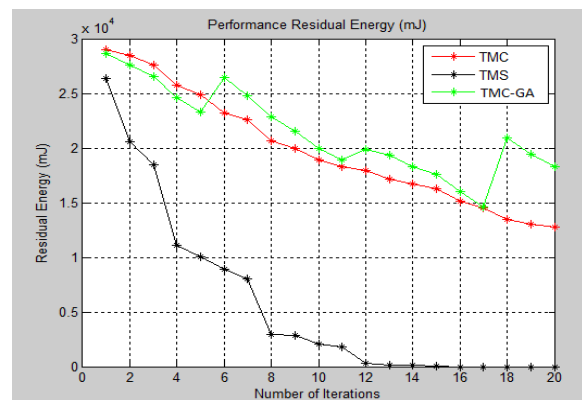


Figure 7. Performance Residual Energy of TMC, TMS, and TMC-GA

### 4.3.5. Routing overhead

Routing overhead is defined as the total routing traffic sent in bits/sec by all the available sensor nodes in the routing network during simulation. In the simulation comparison the defined TMS, TMC and TMC-genetic node recovery algorithm sends a set of control packets to find routes. Routing overhead used to measure the efficiency of the route. Higher the routing overhead more wastage of bandwidth. TMS algorithm uses more bandwidth in terms of routing discovery and updating in the corresponding routing tables. Figure 8 shows the Performance Routing Overhead shows that the TMC and TMC-Genetic node recovery algorithm has less routing overhead than the TMS routing algorithm.

#### 4.3.6. Network lifetime

Network lifetime has defined that availability of network which is directly proportional to the number of alive nodes. Alive nodes directly depended upon the battery energy. When the node battery power starts decreasing which leads to reaching the threshold which turns to the dead node in the network, the dead node may participate in routing discovery but cannot transmit data from one node to another node in the data communication from source to destination.

From Figure 9, TMC algorithm has high network lifetime compared to TMS routing algorithm because TMS keep on decreasing as the number of dead node increases. The better network lifetime depended upon battery power, residual energy, number of alive nodes, and number of hops and total energy consumption of nodes. Figure 9 shows the Performance Network Lifetime shows TMC-Genetic node recovery algorithm is best in terms of network lifetime than the TMS and TMC routing algorithm.

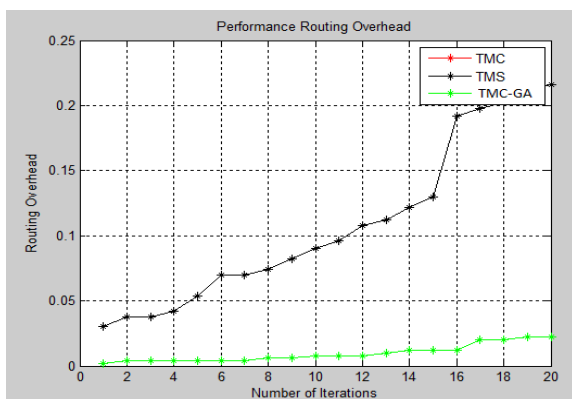


Figure 8. Performance Routing Overhead of TMC, TMS, and TMC-GA

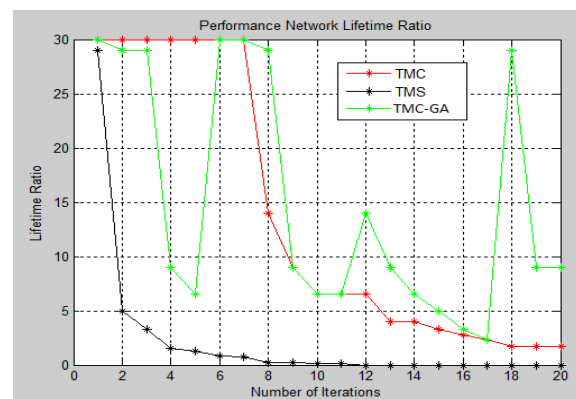


Figure 9. Performance Network Lifetime of TMC, TMS, and TMC-GA.

## 7. CONCLUSION

This paper describes the two algorithms namely TMS algorithm and TMC algorithm. TMS algorithm is used to perform the deployment of the nodes and find the first hop neighbors. From each of the neighbor towards the destination, the routing is performed. The trust is computed for all the routes based on direct trust. Finally, the route which has the highest trust level is picked up. The battery energies of the individual nodes which participate in routing are updated based on distance, the energy required for transmission and energy required for generation. TMC is used to find the route between source nodes to destination nodes. TMC algorithm finds the neighbors of the initiator, the path loss for various noises, trust computation of direct nodes, trust recommendations of neighbors. Finally, the node which has the highest trust is picked up and updates the energy of nodes which participate in routing. TMC-Genetic node recovery algorithm is used to recover nodes whose battery power is shutting down and unable to participate in the data communication. TMC-Genetic node recovery algorithm improves the network lifetime reduces the number of dead nodes and also increase the residual energy of the network.

## REFERENCES

- [1] G. Han, C. Zhang, L. Shu, and J. J.P.C Rodrigues, "Impacts of Deployment Strategies on Localization Performances in Underwater Acoustic Sensor Networks," *IEEE Transactions on Industrial Electronics*, 62(2), 725-1733, 2015.
- [2] S. Climent, A. Sanchez, J.V. Capella, "Underwater Acoustic Wireless Sensor Networks: Advances and Future Trends in Physical, MAC and Routing Layers," *Sensors journal*, 14(01), 795-833, 2014.
- [3] F. Dobsław, T. Zhang and M. Gidlund, "End-to-End Reliability-Aware Scheduling for Wireless Sensor Networks," *IEEE Transactions on Industrial Informatics*, 12(2), 758-767, 2016.
- [4] Jinfang Jiang, Guangjie Han, Lei Shu, Sammy Chan, and Kun Wang, "A Trust Model based on Cloud Theory in Underwater Acoustic Sensor Networks," *IEEE Transactions on Industrial Informatics*, 13(01), 342-358, 2017.
- [5] S. Ganeriwal, L.K. Balzano and M.B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," *2<sup>nd</sup> ACM Workshop on Security of adhoc and Sensor Networks*, 4(3), 66-77, 2006.
- [6] Z.Yao, D.Kim and Y.Doh. "PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security," *IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, 437-446, 2006.
- [7] R. Feng, X. Xu, X. Zhou and J. Wan, "A Trust Evaluation Algorithm for Wireless Sensor Networks based on Node behaviors and D-S Evidence Theory," *Sensors Journal*, 11(2); 1345-1360, 2011.

- [8] Y. Ren, V.I. Zadorozhny, V.A. Oleshchuk and F.Y. Li, "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, 13(7), 1409-1423, 2014.
- [9] A. Boukerche, L. Xu and K. El-Khatib, "Trust-based Security for Wireless ad-hoc and Sensor Networks," *Computer Communications Journal*, 30(11), 2413-2427, 2007.
- [10] R.A. Shaikh, H. Jameel, B.J. d'Auriol, et al., "Group-based Trust Management Scheme for Clustered Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, 20(11), 1698-1712, 2009.
- [11] G. Han, J. Jiang, L. Shu and M. Guizani, "An Attack-Resistant Trust Model based on Multidimensional Trust Metrics in Underwater Acoustic Sensor Network," *IEEE Transactions on Mobile Computing*, 14(12), 2447-2459, 2015.
- [12] M.C. Domingo, "Overview of Channel Models for Underwater wireless Communication Networks," *Physical Communication Journal*, 1(3), 163-182, 2008.
- [13] H.S. Lim, Y.S. Moon and E. Bertino, "Provenance based Trust Worthiness Assessment in Sensor Networks," *7<sup>th</sup> International Workshop on Data Management for Sensor Networks*, 2-7, 2010.
- [14] J. Jiang, G. Han, F. Wang, L. Shu and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, 26(5), 1228-1237, 2015.
- [15] Jiang, Guangjie Han, Chunsheng Zhu, Sammy Chan, and Joel J. P. C. Rodrigues, "A Trust Cloud Model for Underwater Wireless Sensor Networks," *IEEE Communication Magazine*, 55(3), 110-116, 2017.
- [16] LI Juelong, Du Xiaofei, X Jianchun and Y. Qiliang, "Location based Adaptive Routing Protocol for Underwater Acoustic Sensor Networks," *Research Center of Naval Defense Engineering, Beijing*, 1315-1319.
- [17] Haiguang Chen, Huafeng Wu, Jinchu Hu and Chuanshan Gao, "Event-based Trust Framework Model in Wireless Sensor Networks," *In International Conference on Networking, Architecture, and Storage*, 359-364, 2008.
- [18] Youngho Cho, Gang Qu, and Yuanming Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks," *In IEEE Symposium on Security and Privacy Workshops*, 134-141, 2012.
- [19] Guangjie Han, Li Liu, Jinfang Jiang, Lei Shu and Joel J.P.C. Rodrigues, "A Collaborative Secure Localization Algorithm Based on Trust Model in Underwater Wireless Sensor Networks," *Sensors Journal*, 16(2), 229, 2016.
- [20] Tae Kyung Kim, and Hee Suk Seo, "Trust Model using Fuzzy Logic in Wireless Sensor Network," *In International Journal of Electronics and Communication Engineering*, 2(6), 63-66, 2008.
- [21] D. Ramya and Mr. P. Basith, "Design of an efficient Weighted Trust Evaluation System for Wireless Sensor Networks," *In International Journal of Engineering and Computer Science*, vol. 3, pp. 3909-3913, 2014.
- [22] Mohammad Abdus Salam and Alfred Sarkodee-Adoo, "Referencing Tool for Reputation and Trust in Wireless Sensor Networks," *In International Journal of Computer Networks & Communications (IJCNC)*, 7(4), 2015.
- [23] Sunil Kumar, C. Rama Krishna and A.K Solanki, "A Survey on Security Architecture and Key Management Systems in a Wireless Sensor Network," *IJCSNS International Journal of Computer Science and Network Security*, 17(4), 263, 2017.
- [24] James Douglas Hamilton, "Time Series Analysis," 2, 1994.
- [25] D.Li, C.Liu, Y.Du and X.Han, "Artificial Intelligence with Uncertainty," *Journal of Software*, 11, 2004.

## BIOGRAPHIES OF AUTHORS



**Buddesab** received Bachelor of Engineering, Masters of Engineering. He is currently working toward the PhD degree from Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, Bangalore University, India. His research interests include cloud computing, scheduling and resource management, data security and Wireless sensor networks. He is a member of IEEE since 2014. He has published research papers in reputed international journals and conference. He has one year of teaching experience and 4 years of Research Experience.



**Thriveni J.** has completed Bachelor of Engineering, Masters of Engineering and Doctoral Degree in Computer Science and Engineering. She has 4 years of industrial experience and 23 years of teaching experience. Currently she is a Professor in the Dept. of CSE, University Visvesvaraya College of Engineering, Bangalore. She has over 90 research papers to her credit. She has produced four doctorate students and guiding 07 Ph.D Students. Her research interests include Networks, Data Mining and Biometrics.



**K. R. Venugopal** is currently the Vice Chancellor Bangalore University, Bengaluru. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bengaluru. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Micro-processor Programming, Mastering C?? and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE, ACM and ISTE.