EC-STCRA: Energy Conserved - Supervised Termite Colony based Role Assignment scheme for Wireless Sensor Networks

Rajarajeswari. PL*, Karthikeyan N.Kb, Deva Priya. Ma

aDepartment of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore - 641042, Tamil Nadu, India.
bDepartment of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore - 641042, Tamil Nadu, India.

Abstract

Conserving energy and ensuring security are the main challenges of Wireless sensor Networks (WSNs). Energy at the sensors must be preserved to increase the lifetime of the network. Clustering helps in reducing the number of transmissions between the Cluster Head (CH) and the Base Station (BS). In this paper, an Energy Conserved - Supervised Termite Colony based Role Assignment (EC-STCRA) scheme is proposed to conserve energy. The network is trained to provide better performance by incorporating efficient clustering, routing and security schemes. The CHs are randomly selected, and the soldier and the worker nodes are appointed based on their location and Residual Energy (RE). Efficient paths to the BS are found by selecting the worker nodes with high RE. The soldiers protect the network from attacks like Denial of Service (DoS), flooding and spoofing by maintaining an Active List (AL) of reliable nodes along with a Warning List (WL) and a Dead List (DL) of malicious nodes. EC-STCRA outperforms the existing Genetic algorithm (GA) and Ant Colony Optimization (ACO) based clustering and routing schemes in terms of Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), throughput, delay, Residual Energy (RE) and network lifetime.

Keywords: Wireless Sensor Network (WSN); Clustering; Energy Consumption; Routing; Security; Termite Colony Optimization (TCO); Genetic Algorithm (GA); Ant Colony Optimization (ACO).

1. Introduction

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors that monitor the physical or environmental conditions such as temperature, sound, pressure, etc., It is composed of sensing, computing and communication elements that help the observer to perceive and react to events and phenomena in a specific environment [1, 2]. Military applications such as battlefield surveillance inspired the development of WSNs and hence sensors find their applications mainly in areas of monitoring and tracking. Data dissemination between nodes can be either by routing or by flooding [3]. The Base Stations (BS) or Sink nodes have more computational, energy and communication resources. They act as a gateway between the sensor nodes and the end user.

Reducing the number of data transmissions conserve energy in a network. Clustering has proven to be an effective approach for reducing the number of transmissions and organizing the WSN. Besides achieving energy efficiency, clustering also reduces channel contention and packet collisions, yielding improved network throughput even under heavy load. The widespread applications of WSNs and the need for data aggregation demand efficient organization of the network topology to balance the load and prolong the lifetime of the network [4]. In this paper, an Energy Conserved-Supervised Termite Colony based Role Assignment (EC-STCRA) scheme is proposed to increase the lifetime of the network by conserving energy. Routing is the process of selecting the best paths in a network. Multipath routing schemes select alternate paths yielding fault tolerance, increased bandwidth and improved security. Selecting energy efficient paths conserve energy. The
deployment of sensors in an unattended environment and the use of wireless signals as the media of communication make it easy for eavesdroppers to trap the signals. A WSN is highly susceptible to attacks. The limitations in processing, storage, battery lifetime, computational speed and communication bandwidth make the security issues of these networks difficult. The security solutions adopted for Mobile Ad hoc Networks (MANETs) are not directly applicable for WSNs [3]. To ensure secured communication between the nodes in a WSN, authentication of sensor nodes is vital.

2. Termite Colony Optimization (TCO)

Termites communicate by secreting chemical agents called pheromones. The termites recognize their fellow members by sensing the smell on their body. They follow the trail of pheromones left by an individual termite and drop pheromones on their way to the destination [5]. The termites forage for food based on the pheromone trail. Termites move randomly based on the observed pheromone gradient. In the absence of pheromone, a termite moves arbitrarily in any direction. Termite Colony Optimization (TCO) is proposed in [6]. The behavior of termites is analyzed and different types of movement patterns are introduced into the TCO algorithm. They organize themselves based on the principles that play important roles in social behaviors of termites namely, positive and negative feedback, randomness and multiple interactions. The fifth principle, stigmergy is the product of the former four [7]. They build hills by carrying one pebble at a time and pick a pebble if they do not have one. Else, they put their pebble down to get infused with a certain amount of pheromone.

The termites in a colony form a decentralized system and are classified into three groups based on the work they do in the colony namely, reproductives, workers and soldiers. Each individual interacts with each other and their environment. The reproductives are the queens and kings. The workers collect food, feed the termite larvae, soldiers and the queen. The queen acts as a “mother” and forms a colony. There are two ways in which the new royals become heads of the family. When the colony size becomes too large for the royals to govern, some of the sterile alate pairs may not get the hormone secreted by the queen to preserve the alate pairs’ sterile status. These pairs fly out of the colony to form a new colony. The royals in the colony are replaced when the currently reigning queen gradually loses her fertility. This also results in the alate pair gaining fertility. Hence, the most dominant female is chosen as the queen and its mate is made the king. They become the new royals.

3. Related Work

There are many clustering and routing schemes based on Genetic algorithm (GA) and Ant Colony Optimization (ACO). Very little research is done using Termite Colony Optimization (TCO).

3.1 Clustering in WSNs

In the literature, there are many clustering schemes. GA based clustering scheme enables the chromosomes to bring out the best traits in the offspring. Similarly in WSN, the GA based approach helps in balancing the clusters to have equal number of nodes which on the other hand upsurges the energy consumed. Genetic optimization-based clustering protocol has gained some attention [8, 9]. This approach has the advantages of reducing energy dissipation, and enhancing system lifetime, resource allocation and bandwidth reusability. Hurualu et al., [8] have developed a GA based clustering and routing algorithm that chooses an optimal cluster head and minimizes the transmission distance by using a multi-objective function. Bari et al., [10] and Heidari et al., [11] have used GA for clustering. Bari et al., [10] have proposed a GA based routing algorithm using relay nodes for a two-tire WSN. Selection of individuals is carried out using the Roulette-wheel selection method and the fitness function is defined by network lifetime in terms of rounds. For mutation, a critical node
which dissipates the maximum energy while receiving and/or transmitting data is selected from the relay nodes. GA based Mobility Aware Clustering for Energy Efficient Routing (GAROUTE) [12] is a GA based algorithm that is designed to perform energy-efficient mobility-aware clustering for WSNs. The algorithm considers the mobility of each node to dynamically create clusters and evaluates the performance using a free space energy model. Bayraklı and Erdogan [13] have proposed GA Based Energy Efficient Clusters (GABEEC) to optimize the lifetime of WSNs. It involves two phases namely the set-up and steady-state phase. In the set-up phase, static clusters are created with dynamically changing CHs. In the steady-state phase, the nodes communicate with their CHs. A Clustering Based GA (CBGA) that deals with shortening the Traveling Salesman Problem with Neighborhoods (TSPN) route is proposed [14]. It involves a waypoint selection method and GA with an appropriate combination of Modified Sequential Constructive Crossover (MSCX) operator and a mutation operator based on local optimization heuristics of 2-opt developed for TSP.

### 3.2 Routing in WSNs

Gupta et al., [15] have proposed GA based Routing (GAR) to deal with the reduction of energy consumed by minimizing the total distance travelled by the data in every round. As it is based on GA, it finds the solution quickly and computes a new routing schedule based on the current network state. For selection of individuals, it uses tournament selection and the fitness function is defined in terms of the total distance covered in a round. In mutation, the relay node which uses maximum distance to transmit data to its neighbor is selected. Chakraborty et al., [16] developed a GA based protocol called GROUP in which a chain is formed to communicate with the BS. The sensors transmit data to the BS non-periodically, depending on their Residual Energy (RE) and location, thus increasing network lifetime. Badia et al., [17] have propounded Signal-to-Interference Ratio (SINR) based model for scheduling and routing that suits both small and large topologies. Liu et al., [18] have proposed a GA based multi-path energy hole avoidance routing algorithm that selects the numbers of next hop nodes and distributes appropriate proportion of data. It redefines the code, operations and rules of searching optimal solution for the GA to obtain a global optimal solution for flat networks and hierarchical networks. A solution based on Non-dominated Sorting GA (NSGA-II) is proposed in [19] for energy efficient QoS routing in cluster based WSNs. The protocol determines a set of near optimal routes satisfying application-specific QoS parameters in WSNs using elitist NSGA-II. QoS based Energy efficient Sensor routing protocol (QuESt) [20] that uses Multi-objective Optimization using non-dominated sorting in GA (MOGA) is proposed in [21] to find paths in a flat (non-clustered) WSN.

A centralized power efficient routing algorithm called Energy Harvesting Genetic-based Unequal Clustering-Optimal Adaptive Performance Routing algorithm (EHGUC-OAPR) is proposed in [22]. The BS uses EHGUC algorithm to form clusters of unequal sizes and select associated CHs in which the clusters closer to the BS have smaller size. The BS adopts OAPR algorithm to construct an optimal routing among each CHs. Ant Colony Optimization (ACO) algorithms are applied to solve various optimization problems effectively. The dynamic adaptability and optimization capabilities of ACO help in finding optimal paths to the sink. Ye and Mohamadian [23] have proposed a dynamic clustering based routing algorithm that uses ACO to increase the lifetime of sensors. Each sensor node is considered as an artificial ant and dynamic routing is exhibited as ant foraging. The ants generate pheromone on finding an energy efficient channel from the source to the sink. Route discovery, data aggregation and information loss are modeled as the processes of pheromone diffusion, accumulation and evaporation. The RE in each node is considered and the probability of selecting an optimal channel for extending the lifespan of WSNs is found. Du and Wang [24] have propounded an uneven clustering routing algorithm for WSNs based on ACO. It considers the distance between the CHs and the sink to determine the size of the cluster. To preserve energy during inter-cluster data forwarding, the clusters near the sink are smaller than the ones farther from the sink. Based on the Received Signal Strength (RSS), the distance to the sink is calculated.
In [25], a distributed ACO based routing algorithm for data aggregation is proposed. It finds an optimal path to the sink and uses the positive feedback of ant algorithm for data collection. The Ant Colony-based wireless sensor network Routing Algorithm (ACRA) proposed in [26] uses the primary and alternate path by considering the impact of pheromone. In [27], PARA that considers the energy level and distance of transmission is proposed. An ACO based routing scheme that uses the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol to route the data packets and maximize energy efficiency is proposed for WSNs [28]. The ant agents placed at the source node use an iterative probabilistic approach along with the pheromone value to find an optimum path to the sink.

Zhang et al., [29] proposed Sensor driven and Cost-aware ant routing (SC) in which it is assumed that ants have sensors to smell food at the beginning of the routing process so as to predict the best direction for the ant. Each node stores the cost to each of its neighbors, the cost to reach the destination and their respective probability distributions. The algorithm might produce misleading solutions due to the obstacles on the path. If the ants are not able to predict the destination or the cost, the SC protocol becomes basic ant colony routing and the network is travelled around to find the destination. They extended their work and proposed Flooded Forward ant routing (FF), where the misguidance of ants due to the obstacles or moving destinations is considered and the protocol is based on flooding of ants from the source to the sink. The system does not yield better performance when the system density is high.

Ghasemaghaei et al., [30] introduced Many-to-One Improved Ant Routing (MO-IAR), in which the algorithm establishes the shortest path using the ant agent in the first phase and performs routing in the second phase. It involves a proactive mechanism to control congestion. Kumar et al., [31] have proposed an ant-based QoS routing protocol for heterogeneous WSNs involving scalar and multimedia sensor nodes with diverse QoS requirements. Different path selection criteria are defined for control traffic and data traffic and the QoS routes are selected based on the types of traffic. Okazaki and Frohlich [32] have introduced Ant-based Dynamic Zone Routing Protocol (AD-ZRP), a self-configuring reactive routing protocol for WSNs. It is based on HOPNET, a multi-hop and self-configuring hybrid routing protocol based on ACO and Zone Routing Protocol (ZRP) for MANETs. They extended their work [33] by proposing an Ant-based Dynamic Hop Optimization Protocol (ADHOP), a self-configuring reactive routing protocol for dynamic WSNs. ADHOP with ACO deals with the restrictions of WSNs and improves route discovery and route maintenance using pheromone.

Adaptive Ant Colony System (AACS) proposed by Li and Shi [34] is a data-centric routing protocol that uses Direct Diffusion (DD) to distribute the interest messages and applies the AACS algorithm to construct the Minimum Steiner Tree (MST). Novel ACO-based Routing Protocol (NARP) proposed by [35] uses the principles of ACO routing to solve the optimization problem. NARP computes the control factor of the decision probability by combining the ratio of the RE and the total energy with the distance of any two nodes. The incremental equation of pheromone considers the length of data packets and the hop-size between the source node and the destination node. Forward ANT (FANT) explores the paths of the network and Backward ANT (BANT) establishes the path information acquired by the FANTs. A study of artificial termites that deals with routing in sensor networks is discussed in [36].

4. Energy Conserved - Supervised Termite Colony based Role Assignment (EC-STCRA) Scheme

Energy plays a vital role in a WSN. Energy Conserved - Supervised Termite Colony based Role Assignment (EC-STCRA) scheme is proposed to conserve energy by assigning roles to sensors in a network. It implements the TCO algorithm to deal with the three main issues in WSN namely, Energy, Routing and Security. The nodes are organized as clusters with CHs, Worker/Forwarding nodes and Soldier nodes. The CHs help in reducing the energy consumption, workers aid in routing and provide reliable communication and soldiers protect the network from the malicious activities of intruder nodes. EC-STCRA includes the following steps namely, cluster formation, energy conserved routing and providing history based security.
4.1 TCO based Clustering

In TCO approach, the queens are not leaders. They help in forming and managing a colony. Similarly in a WSN, the CHs manage clusters. They do not dominate the workers and soldiers, but coexist with them. Based on the TCO approach, the sensors take up the roles namely, Cluster Heads (Royals and alates), normal sensor nodes (workers) and security agents (soldiers). Initially, the CHs are chosen based on the distance between the BS and the node selected as the CH. The CHs are dynamically chosen based on the RE. If the RE of a CH goes below a threshold, then a new CH is selected. When a sensor node receives HELLO messages from CHs, it compares the Received Signal Strength Indicator (RSSI) of messages. It chooses the CH with high signal strength. If the signal strength is weak from all CHs, then the message is discarded and the receptor node waits to join another CH. Usually, the soldiers are the ones at boundary of the network. The workers are the normal sensors which sense the events and forward them either directly to the soldiers or indirectly through multiple hops. The worker nodes become soldiers if they detect a malevolent activity. The CHs are dynamically chosen based on energy and distance between the node and the event. If there are no events to trigger the network, then the nodes go to sleep mode gradually from the opposite location where the recent event occurred.

4.2 Residual Energy based Routing (RER) scheme

Data transmission in a WSN can either be single hop or multihop. In the case of single hop communication, the sensor nodes send the sensed data to the CH directly. In multihop data transmission, the sensed data reaches the CHs through a number of hops. The main challenge in WSN is designing an energy efficient, scalable, robust and adaptable routing protocol better than the existing state-of-the-art routing protocols. WSN is similar to a termite community [1, 36]. Alternate solutions are applicable in a technical network but not in a biological community [37, 38]. Like the termites, the sensors organize themselves and provide solutions based on the individual behavior of each node [7, 39]. When the termites go in search of food, the pheromone trail that is generated is the shortest route to the food source and hence highly optimized. Finding shortest paths is not an apriori goal of TCO. The shortest path may not be energy efficient. The pheromones are hormones secreted by termites for food foraging and self-defense. These pheromones help in identifying paths in the future. Though the paths dissolve after sometime, using them for the succeeding transmissions makes them vulnerable to attacks. Just as the termites find the food source easily and renew the pheromone trail, communications between the same source and destination establish the paths.

In this paper, termite agents are implemented to find the energy efficient paths by considering the energy of the neighboring termite nodes. The total path energy should be minimum. Reducing the number of nodes along the path to the sink will not help in conserving energy. This may lead to energy depletion at some nodes, leading to network partitioning. In the proposed Residual Energy based Routing (RER) scheme, to ensure security and reduce the total energy along the path, the next hop node with high energy reserve is selected for transmission. Since the nodes are chosen dynamically, energy drain due to recurrent usage of nodes reduce to a greater level. This ensures security as the intruder will not be able to predict the path to the BS.

4.2.1 The Pheromone Table

The pheromone table keeps the information about the Routing Factor (RF) computed based on RE and RSSI at time ‘t’. The rows correspond to the values of the destinations and the columns to that of the neighbors.

\[
RF_{i,j}^t = RE_i^t \cdot RSSI_{i,j}^t
\]  

(1)
The entries in the pheromone table are referenced as ‘RF$_{ij}$’, where ‘$i$’ is the neighbor index and ‘$j$’ is the source. The neighbor with high ‘$RF_{ij}$’ is selected as the next hop node. As the distance increases, the RSSI decreases. The amount of energy taken for transmission increases, which on the other hand decreases the RE. Let the energy loss rate be ‘$\varphi$’. A high loss rate reduces the amount of RE to a greater extent, while a low value degrades the RE slowly. The RE loss interval is considered to be one ms, which is called the decay period.

$$RF_{ij}^t = RF_{ij}^{t-1} * e^{-\varphi}$$  

Equation (2)

The RF update table for node ‘C’ in a sample WSN is shown in Fig. 1. To ensure robustness and flexibility, some applications need a slow decay rate, and some applications like security and target tracking applications need fast decay process. The value of ‘$\varphi$’ and ‘$x$’ in equation (3) varies with the application. To account for the energy loss, each value in the RF-Pheromone table is periodically subtracted by the percentage of the original value as shown in equation (3). At each cycle of the algorithm, the fitness value of each termite (sensor) is evaluated. The fitness value is used for computation of pheromone (RF) content at each location of termites. The pheromone content at a location is computed based on the following equation:

$$RF_{ij}^t = (1 - \varphi) RF_{ij}^{t-1} + \frac{1}{\text{FITNESS}(i)+1}$$  

Equation (3)

where ‘$\varphi$’ is the evaporation rate that is taken in range of [0..1], ‘$RF_{ij}$’ and ‘$RF_{ij}^{t-1}$’ are the RF levels at the current and previous locations of $i$:th termite. Each node maintains a table keeping in store the amount of RE of each neighbors.

4.3 Security

Many schemes available in the literature consider the attacks from outside but fail to identify the malevolent behaviour of the nodes in the network. The malicious nodes in a network are to be recognised and circumvented so as to overcome the attacks from inside a network. An intrusion detection system is a system that dynamically monitors the events taking place in a system and decides whether these events are symptoms
of an attack or constitute a legitimate use of the system. While trying to ensure security, the challenges of limited amount of resources like energy, processing capacity and storage are to be taken into account.

In general, the intrusion detection schemes are categorized into misuse intrusion detection schemes and anomaly intrusion detection schemes. The anomaly schemes are classified into

- **Supervised** - Trains the detection model which requires prior knowledge about the normal and anomalous behaviour. e.g., Rule-based intrusion detection schemes.
- **Semi-supervised** - Has knowledge of either normal or the anomalous class that aids in building a model for detection.
- **Unsupervised** - Does not require any prior knowledge to build the detection model. Instead uses some measurements to decide whether the data instance is normal or anomalous.

The scheme proposed in this paper is a supervised model. The security solutions proposed in the literature can be grouped into two main mechanisms namely, prevention based mechanisms and detection based mechanisms. The proposed scheme is a combination of both.

### 4.3.1 History based Security (HS) Scheme

The pheromones secreted by the termites are also used to ensure security in a colony. The smell of pheromones is unique to each species and differs based on the situations in which they are secreted. The soldier termites protect the colony from ants and other animals which hunt the termite colony for food. When the attackers find a colony, they attack the termite soldiers stationed at the boundary of the colony. The other soldier termites guard the royals and young ones. When there is an attack, the termites at the boundary of the colony send a kind of pheromone, the smell of which when breathed by other termites of the colony helps them to recognize the attack. More soldier termites are sent for the protection of the colony. The sensitive WSN applications like military are prone to attacks. The intruder is very much concerned about the CH (Royal) than other nodes in the network. Taking hold of a CH is equivalent to capturing a group of nodes, may be in hundreds. The soldiers defend the CHs and also forward the data received from the workers to the BS and vice versa.

In the proposed History based Security (HS) scheme, when a soldier node senses a malicious activity at a worker node, it discards it. It sets a boundary between the CH and the workers. The CH is thus protected from malevolent activities. The behavior of nodes in the previous time slots is analyzed and the decision is taken by the soldiers to circumvent these vindictive nodes. HS overcomes flooding, Denial of Service (DoS) and spoofing attacks. All the worker nodes that are active are added to the Active List (AL). The nodes anticipated to be vindictive are put into the Warning List (WL). If the misbehavior of a node is confirmed to be malicious, it is added to the Dead List (DL). All the communications to and from the node are discarded.

The aim of the flooding attack is to exhaust the network resources by consuming a node’s resources such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. A malicious node can send a large number of Route REQuests (RREQs) in a short period to a destination node that does not exist in the network. As no node responds to these RREQs, these RREQs flood the whole network. This leads to draining of the node battery power leading to Denial of Service (DoS). In this work, a Flood Count based on the number of neighbors is set to overcome the flooding and hence the DoS attack. If the frequency of packets received is more than a Threshold (τ) from a next hop node, then the soldier drops the packets and does not forward to the CH. This reduces the overall traffic in the network. ‘τ’ is determined based on the number of next hop nodes at a particular instant of time. Each sensor is given a unique ID. The royals and the soldiers are aware of the nodes in the network. It is the responsibility of the soldier to identify spoofed ID. If such an ID is found, the soldiers drop the packets and do not forward the packets received from them to the CHs (royals). Since the nodes switch roles only when needed, energy is highly conserved. Fig. 2 shows the steps involved in the proposed scheme.
for $i = 1$ to $N$  
   // **Compute fitness of the termites**
   \[ RF^{(i)}_{L_j} = (1 - \varphi) RF^{(i-1)}_{L_j} + \frac{1}{\text{FITNESS}(i) + 1} \]
end for

for $i = 1$ to $N$  
   // **Find the best neighbor**
   \[ RF^{(i)}_{L_j} = RF^{(i-1)}_{L_j} * e^{-\varphi} \]
   Find the neighbors of Sensor (Termite) ‘$i’
   If termite ‘$i’ has neighbors then
      Select the neighbor with high RF
   end if
end for

for $i = 1$ to $N$  
   // **Finding malicious activity**
   if any malicious activity of a termite is detected
      Add the termite to Warning List
      if the malicious activity is confirmed
         Add the termite to Dead List
      end if
   end if
end for

![Fig. 2. Algorithm](image)

### 5. Results and Discussion

The system is implemented using ns2. Initially the CHs are selected based on the distance between the sensor nodes and the BS, which is determined by the RSSI value of the HELLO packets received by the node.

<table>
<thead>
<tr>
<th>PARAMETERS</th>
<th>VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing protocol</td>
<td>SC, FF, AODV, Termite-hill</td>
</tr>
<tr>
<td>Number of CHs, Soldiers, Worker nodes</td>
<td>100</td>
</tr>
<tr>
<td>Transmission range</td>
<td>35 m</td>
</tr>
<tr>
<td>Data traffic</td>
<td>Constant Bit Rate (CBR)</td>
</tr>
<tr>
<td>Initial Energy</td>
<td>3.4 J</td>
</tr>
<tr>
<td>Tx Power, Rx Power, Idle Power, Sleep Power</td>
<td>0.33 J, 0.1 J, 0.05 J, 0.03 J</td>
</tr>
<tr>
<td>Simulation time</td>
<td>20 ms</td>
</tr>
</tbody>
</table>

The CH from which the maximum signal strength is detected is chosen as the CH of the node. The simulation parameters are listed in Table 1. The energy expended for each packet transmission is calculated and detected from the sensor node. When the energy level of a CH goes below 30%, then a new CH with more RE is randomly chosen. The performance of the proposed work is compared with ACO and GA based systems. The proposed TCO based system yields better results. EC-STCRA yields 24.09% and 12.7% better throughput when compared to ACO and GA based schemes (Fig. 3). The PDR of ACO and GA based schemes are 21.74% and 9.79% less in contrast to EC-STCRA (Fig. 4). EC-STCRA yields 2.66 and 2.11 times less PLR when compared to ACO and GA based schemes (Fig. 5). The proposed EC-STCRA scheme conserves energy. The
RE of ACO and GA based schemes are 25.97% and 11.26% high in contrast to the propounded scheme (Fig. 6).

![Fig. 3. Throughput](image1)

![Fig. 4. Packet Delivery Ratio](image2)

![Fig. 5. Packet Loss Ratio](image3)

![Fig. 6. Residual Energy](image4)

![Fig. 7. Delay](image5)

![Fig. 8. Routing overhead](image6)

ACO and GA based schemes involve 61.32% and 42.97% more delay in contrast to the proposed EC-STCRA scheme (Fig. 7). ACO and GA based schemes involve 1.54 and 1.99 times more routing overhead when compared to the EC-STCRA scheme (Fig. 8). Table 2 shows the performance of the schemes. The performance improvement is shown in terms of percentage for all the parameters except PLR and routing overhead.
### Table 2: Performance Comparison

<table>
<thead>
<tr>
<th>TIME (ms)</th>
<th>THROUGPUT (KB)</th>
<th>PACKET DELIVERY RATIO (%)</th>
<th>PACKET LOSS RATIO (%)</th>
<th>RESIDUAL ENERGY (J)</th>
<th>DELAY (ms)</th>
<th>ROUTING OVERHEAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACO</td>
<td>GA</td>
<td>TCO</td>
<td>ACO</td>
<td>GA</td>
<td>TCO</td>
</tr>
<tr>
<td>2</td>
<td>2685</td>
<td>2920</td>
<td>3245</td>
<td>81.79</td>
<td>88.41</td>
<td>95.43</td>
</tr>
<tr>
<td>4</td>
<td>2596</td>
<td>2831</td>
<td>3156</td>
<td>80.68</td>
<td>87.3</td>
<td>94.32</td>
</tr>
<tr>
<td>6</td>
<td>2529</td>
<td>2764</td>
<td>3089</td>
<td>78.14</td>
<td>86.11</td>
<td>93.13</td>
</tr>
<tr>
<td>8</td>
<td>2407</td>
<td>2642</td>
<td>2967</td>
<td>74.88</td>
<td>84.76</td>
<td>91.78</td>
</tr>
<tr>
<td>10</td>
<td>2326</td>
<td>2561</td>
<td>2886</td>
<td>73.6</td>
<td>81.5</td>
<td>90.31</td>
</tr>
<tr>
<td>12</td>
<td>2285</td>
<td>2520</td>
<td>2845</td>
<td>73.12</td>
<td>80.22</td>
<td>88.52</td>
</tr>
<tr>
<td>14</td>
<td>2186</td>
<td>2421</td>
<td>2746</td>
<td>70.68</td>
<td>79.74</td>
<td>87.24</td>
</tr>
<tr>
<td>16</td>
<td>2137</td>
<td>2372</td>
<td>2697</td>
<td>69.57</td>
<td>77.3</td>
<td>86.76</td>
</tr>
<tr>
<td>18</td>
<td>2052</td>
<td>2287</td>
<td>2612</td>
<td>66.75</td>
<td>76.19</td>
<td>84.32</td>
</tr>
<tr>
<td>20</td>
<td>2035</td>
<td>2270</td>
<td>2595</td>
<td>65.92</td>
<td>73.67</td>
<td>83.21</td>
</tr>
<tr>
<td>AVERAGE</td>
<td>2324</td>
<td>2559</td>
<td>2884</td>
<td>73.51</td>
<td>81.52</td>
<td>89.50</td>
</tr>
<tr>
<td>PERFORMANCE IMPROVEMENT</td>
<td>24.09</td>
<td>12.70</td>
<td>21.74</td>
<td>9.79</td>
<td>2.66</td>
<td>2.11</td>
</tr>
</tbody>
</table>
6. Conclusion

In this work, an energy efficient TCO based role assignment scheme that deals with clustering and routing in WSNs is proposed. This scheme outperforms the GA and ACO based schemes in terms of the amount of Residual Energy (RE), Packet Delivery Ratio (PDR), throughput, Packet Loss Ratio (PLR), network lifetime and the delay involved. It overcomes various attacks like DoS, spoofing and flooding. An energy efficient path is established by considering the RE of the neighboring nodes. The CHs are dynamically selected based on the energy reserve and they are fortified from any malicious activity. Further, the network is pruned by discarding vindictive nodes.

References


