Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.027545
Article

Tech Science Press

Efficient Hybrid Energy Optimization Method in Location Aware Unmanned WSN

M. Suresh Kumar[1,*] and G. A. Sathish Kumar[2]

[1]Department of CSE, Sri Venkateswara College of Engineering, Sriperumbudur, 602117, India
[2]Department of ECE, Sri Venkateswara College of Engineering, Sriperumbudur, 602117, India
*Corresponding Author: M. Suresh Kumar. Email: sureshm@svce.ac.in

Received: 20 January 2022; Accepted: 06 March 2022

Abstract: The growth of Wireless Sensor Networks (WSNs) has revolutionized the field of technology and it is used in different application frameworks. Unmanned edges and other critical locations can be monitored using the navigation sensor node. The WSN required low energy consumption to provide a high network and guarantee the ultimate goal. The main objective of this work is to propose hybrid energy optimization in local aware environments. The hybrid proposed work consists of clustering, optimization, direct and indirect communication and routing. The aim of this research work is to provide and framework for reduced energy and trusted communication with the shortest path to reach source to destination in WSN and an extending lifetime of wireless sensors. The proposed Artificial Fish Swarm Optimization algorithm is used for energy optimization in military applications which is simulated using Network Simulator(NS) tool. This work optimizes the energy level and the same is compared with various genetic algorithms (GA) and also the cluster selection process was compared with the fission-fusion (FF) selection method. The results of the proposed work show, improvement in energy optimization, throughput and time delay.

Keywords: Wireless sensor networks (WSNs); optimization algorithm; routing algorithm; military applications

1 Introduction

Recently, Wireless Sensor Networks (WSNs) are picking up unmistakable quality in the household, modern and military applications, for example, brilliant homes, home computerization, Internet of Things (IoT), shrewd urban areas, machine-to-machine correspondence, natural checking, observation applications and so forth. WSNs are [1] comprised of countless little, sensors and ease gadgets (or hubs) that are fit for detecting and correspondence with restricted assets regarding memory, preparing and vitality. The primary target of hubs in the system is to detect or gather the information identified with a procedure or a situation and report it to a sink hub (or Base Station) with helpful directing choices. Revealing the information from every hub legitimately to the Base Station (BS) isn't attainable consistently in view of constrained transmission extend. The amazing qualities of WSN cause it to have an expansive application prospect in military safeguard, natural observing, organic, restorative, catastrophe help and business applications, etc. The topology conventions of WSN ordinarily center on how to isolate the entire system into bunches and how to make multi-bounces development among these groups sets out toward moving sensor information to the base station without anyone else association. For WSN, a noteworthy time is spent during the building of system topology to guarantee the security of the correspondence. As of late, individuals have advanced diverse security steering conventions. In the writing, a subset of sensor hubs offers boundary inclusion over a zone of intrigue if the sensor hubs are apportioning the zone into two locales with the end goal that any item moving starting with one area then onto the next is destined to be perceived by a sensor hub [2]. There are various noteworthy uses of obstruction inclusion for instance interruption identification and thusly it has pulled in heaps of contemplations as of late [3].

An intrusion detection system (IDS) [4] attempts to see the risks conditions of structures in the setting of the risky ambushes, paying little character to whether these strikes have not been experienced start at now. Impedance is a technique for exercises that can impact unapproved access or change of the remote framework structure. IDS parts can see unsafe gate crashers in the setting of those blends from the standard and screen the PC frameworks and structures, seeing possible impedances in the structure and startled customers after deterrents had been seen, reconfiguring the structure if this is conceivable [5]. Everything considered the neighbors of a stunning obsession point are the central pieces taking in those shocking practices. In this way, it is helpful to draw in each inside to screen its neighbors to such a degree, to the point that IDS instruments can be influenced as vivacious as time stipends [6]. IDS watches and researches the events made in the framework structure to see the most stunning security issues and it is used to screen the structure to audit anything striking. There are two key strategies for perception for IDS are squash zone [7] in the setting of models, these statutes will check for marks on the framework and appropriately structure assignments attempt to get got a handle on strike that should be considered as mistreating. Ponder embracing [8] relies on the standard direct of a structure and it pulls back standard activities against watched events to see supervisor deviations.

In the present years, undeniable IDSs have been proposed for WSNs. IDSs filling in as the second line of the reason behind fundamental are major in giving an astoundingly secured information structure and it can sensibly watch potential gate crashers and from this time forward give all-around accreditation [9]. The zone models are single-seeing clear request and specific seeing verification used to see the square in both homogeneous and heterogeneous WSNs by portraying impedance divulgence probability concerning the tangle separated and the structure parameters [10]. IDS for WSN are ace through the examinations and plan of a dynamic structure with the specific framework to pick better speculations against various checks [11]. The perfect approach joins the holding tight customer accreditation and IDSs in a coursed approach to managing direct oversee control assemble revealed major the issue as a POMDP [12] multi-regulated criminal issue. A dynamic trust connection custom [13] using the using get-together to change as appeared by a wide number of heterogeneous structures for flexibility and to fit in with uneven or beating framework for survivability and impedance security [14] A kept estimation, named as Localized Minimum Weight Barrier Protocol (LMWBP) [15] gives a general most close off point to luxuriously process the trust levels in the structure with high thickness risky ambushes [16,17]. WSNs help in military tasks by passing on fundamental data rapidly and dependably to the opportune individual or relationship at the ideal time, along these lines fundamentally improving the effectiveness of battle activities. Here, it was utilizing the wireless sensor network for checking and following application in military field was discussed [18]. Security is a significant worry right now. First, it is necessary to list the arrangement of utilizations in the military field and what are the various types of attacks right now. Later, the answers for basic types of attacks in military application to be discussed. Different techniques are utilized to mislead the assailant from getting the data [19]. The unmanned vehicle is joined in the military application to make the system progressively make sure about and improve the existence time and availability of the network. The vehicle will be furnished with a mote controlling the vehicle dependent on base station directions and encompassing hubs data [20]. This work has proposed solutions for the significant sorts of assaults in the military field. The unmanned vehicle can be utilized to check the unwavering quality and honesty of the network. The rest of the manuscript is organized as follows: Section 2 is related works and Section 3 is problem and contribution. Section 4 is simulation and discussion of proposed work and finally, Section 5 is the conclusion and future enhancement.

2 Related Works

A lot of investigators had been industrialized intrusion detection in WSNs. Among them some of the works are analyzed here; Han et al. [21] have proposed information against sinkhole attack (IDASA) estimation proposed to see sinkhole center focus interests. IDASA count joins two phases are seeing suspicious obsession centers, seeing sinkhole centers and expelling sinkhole centers. The seeing suspicious obsessions are plots the controlling approaches to manage regulate facilitate control see suspicious obsession centers as showed up by the measure of the sensor make hands over the light of a planning way. The sinkhole center is used to detect disturbances from suspicious troubleshooting by using support between plot times and two-letter sensors. Duan et al. [22] have introduced a game-theoretic technique-based energy-aware secure data transaction in WSNs. To reduce the overhead, the game-theoretic approach is utilized and also the trust of each node is calculated. Then, finally, the trust-based secure transaction is done. The simulation results were clearly indicated the performance of the proposed methodology.

Similarly, Ahmed et al. [23] have exhibited Trust and Energy Efficient Routing Protocol (TERP) that utilizes an appropriated trust model for the location and disconnection of getting rowdy and defective hubs. Additionally, TERP consolidates a composite directing capacity that incorporates trust, lingering vitality and jump include of neighbor hubs in settling on steering choices. This multi-aspect directing system adjusts vitality utilization among confided in hubs while steering information utilizing shorter ways. The re-enactment results show diminished vitality utilization, improved all through and arrange lifetime of TERP. In [24], Huang et al., have introduced IDs using an HSOM neural network. It is used to gain change takes after and see impedances and a dynamic modifying approach to manage administer coordinate distribute with the issue of titanic and imbalanced designing data. An advancement show is made to depict the dynamic properties of the structure advance. With the assistance of this movement shows up, the level of getting ready to set used for move setup studying can be basically decreased.

Zhang et al. [25] have developed intrusion detection using IDSHT. This model has versatility and fitting for tirelessly shifting WSNs laid out by changes in the perceptual condition, advances of conditions of center obsessions and groupings set up stock in regard. A multidimensional two-level dynamic trust formation in the stage of sensor centers and assembling heads considering smart trust, consistency trust and substance trust is moved, which joins design examination and information-based appraisal in the settled skip make. This deciphers trust is pondered and trust is surveyed by neighbors and base stations. The deterrent area part in light of a self-adaptable dynamic trust edge is delineated out to empower the adaptability and centrality and is sensible for mean-based WSNs. Ahmed et al. [26] propose a lightweight solution for asset obliged sensor nodes that neither force an excessive number of limitations for network activity nor require any particular arrangement of assets for the trust-aware routing protocol. Similarly, Sedjelmaci et al. [27] have proposed ids and ejection framework against lethal attacks, which sees savage ambushes with high accuracy before they hurt the structure while thinking about the shocking position preventions of different obsession centers. The security redirection issue is controlled by a Bayesian beguilement plot. It is other than made by the IDS and attackers with the outline of impedance release structure (IES) and suspicious obsessions, where each one of them finishes particular approaches to help their own particular settlements.

Additionally, Rajeshkumar et al. [28] analyzed an IDS based on TRAACK in WSN and Kalman filter to predict the trust of the node. The simulation section clearly shows the effectiveness of this method. Santoro et al. [29] have proposed hybrid network intrusion detection systems (NIDS) using DEMPSTER-SHAFER (DS) theory to sympathetically watch mastermind allocator vector (NAV) ambushes. The high certification rate execution has been made signature-based NIDSs close to the noticeable strikes given by the assortment from the standard-based NIDSs. The zone justification ties the mix of evaluations from different estimations over various layers of learning with a particular monster focus to settle on a total decision on whether a NAV get happens or not. Alsaedia et al. [30] have proposed an Energy Trust System (ETS) to viably distinguish Sybil attacks, which uses multi-stage clear insistence in the setting of character and position bolster. A trust figuring is connected in the setting of the centrality of every sensor center point. Data indicate is used to diminish correspondence overhead and extra centrality. The execution of this structure is poor down the degree that security and resource use using theoretical and redirection-based procedures. Moreover, Gabriel et al. [31] have presented the k-barrier coverage-based IDs. For detection, sensor density, sensor and intruder density are considered.

The hybrid energy optimization of the unmanned method consists of five processing steps as the proposed system model, clustering of nodes in a heterogeneous environment, trust aware recommendation, routing and optimization. Many works have been introduced for energy optimization for the different wireless environments and a few works are as follows. Cognitive Unmanned Aerial Vehicle(UAV) systems application has been introduced for energy optimization and detected data size of communicated message [32]. The objective of this work was that minimize the time to transmit the data since the battery of the UAV is insufficient. The drawback of this work was that introduced propulsion energy and interference so these consumed energies unnecessarily. Here the following concepts have to be explored and these concepts dealt with system model for optimized energy usage, clustering mechanism for the heterogeneous environment, unmanned application-oriented trust aware recommendation system and finally optimized routing in WSN environment.

The following works dealt the system model for optimized energy usage. A V-Detector-based Intrusion Detection system was proposed using a negative selection algorithm (NSA) [33]. This system model was used to reduce the energy for computation and storage systems. This work working based on three-level detection mechanisms. This work enhances the detection feature using principal component analysis. Mature and memory detection sets are arranged and participate in intrusion detection in the WSN environment. V-Detector was also played a vital role in finding second attacks, increased detection rate and quick responses. For IoT-based WSN like Smart vehicles, smart industries and smart homes the dynamic sensing rate and mobile sink deployment were essential. The work was proposed for improving dynamic sensing rate and mobile sink deployment using Q-Learning based Cooperative network model system [34]. There will be information loss if not proposed Q-Learning algorithm for clustering using sink deployment for achieving better sensing rate. the working mechanism of this proposed work that to reduce buffer overflow and information loss for sink deployment a method is proposed to find the adaptive half time. A converging analysis has been introduced to measure variable sensing rates. This system improvised the lifetime for medium-scale WSN based smart system and numeric evaluation and reduced considerable energy.

A system model for WSN using adapting sensor used framework has been proposed [35] and it has the additional feature as learning to sense multi-sensing WSN. This work was upper confidence bound algorithm was used in the measurement cycle to select the optimal active sensor set. And this selection will be helping measure the energy consumption of sensors and the availability of energy in networked nodes. To perform this, work a model system called Gaussian process-based prediction strategy has been handled. This model system measures the cross-correlated parameter among active and inactive sensors. This work has been checked with the real-time application of air pollution monitoring and gathered sample rate and has achieved 54% energy efficiency additionally with efficacy and efficiency parameters. Tab. 1 listed the system models proposed for WSN with various secure and IoT applications.

Table 1: System model based applications

S. no	System model	Work for	Additional feature and method
1	V-detector based IDS	Finding second attack, quick response and detection rate in IDS	NSA as method used reduce energy consumption in computation and storage
2	Cooperative network model	IOT based Smart application in which achieve efficient sensing rate and sink deployment and buffer overflow and adaptive half time	Q-Learning based algorithm for measure efficiency of sink deployment and sensing rate
3	Adaptive sensor used framework	Air pollution monitoring and achieved less energy consumption for active sensors	Upper confidence bound algorithm and Gaussian process based prediction strategy

Clustering mechanisms for the heterogeneous environment and its applications are carried out in many types of research. Usually, efficient data gathering in distributed WSN based applications, clustering algorithms are used. One of the works related to such a concept was introduced using hierarchical protocols-based clustering [36]. The work was to save energy cluster nodes to be selected with higher remaining energy concept and further to send collected data to the base station. Enhanced clustering hierarchy as method proposed which solve redundant data transmission using the sleepwalking mechanism. This mechanism could solve overlapping and neighbor node redundant node data collection and hence maximize the lifetime of the network. The proposed solution was implemented to check the effectiveness the efficiency of data collection and transmission. An energy-efficient clustering algorithm was discussed to transmit data in WSN and this work was identified as LEACH clustering algorithm [37]. This work was also discussed and compared with EEUC, HCC and PEACH. The performance measures compared were average throughput, the energy efficiency of packet delivery and the lifetime of the network. This work was also sent encrypted data over the WSN network by introducing Cluster Head (CH). An efficient clustering algorithm with the heterogeneous nodes-based network for radio sensor networks was proposed to adopt low energy adaptive clustering hierarchy [38]. In this work the heterogeneous-based LEECH (HLEECH) proposed and based on sink node broad caste message about average cluster radius and an optimal number of cluster head, HLEECH finds the CH based on radius competition. Using this sink information, energy-efficient CH formed every time. This mechanism using experiment, it was observed that it produced a maximum of energy utilization efficient for radio cognitive network as per deployment cost. Tab. 2 is listing the clustering mechanism for a heterogeneous based WSN network.

Table 2: Heterogeneous based network's clustering mechanisms

S. no	Clustering name	Mechanism	Performance
1	hierarchical protocols-based clustering	Higher remaining energy first	data transmission energy efficiency
2	LEACH	Random based CH selection	Packet delivery ratio of network, average throughput and energy efficiency of packet delivery
3	HLEECH	Sink broad caste message	Maximum energy utilization efficiency

The optimal routing algorithm for WSN is essential to reduce consumption energy. Energy consumption for routing is majorly based on the scale of the network and topology which was adapted. A work-related to efficient routing was proposed with multi-level heterogeneous routing with learning Automata and an opportunistic shared spectrum was used as an application [39]. A method is called learning automata-based multilevel heterogeneous routing proposed for cluster head selection. The cognitive radio spectrum was used in the base station to select the Cluster heads. A single-hop network of Different Sensor networks was used as multi-hop network. Various categories were implemented and these were super-advanced, super intermediate and intermediate categories. The performance parameter used here were network lifetime and stability and 10% efficiency achieved as compared to the existing scheme for routing. A routing algorithm for heterogeneous energy with traffic-aware sleep cluster proposed for WSN. In this work, an energy and traffic-aware sleep-awake (ETASA) protocol was proposed [40]. A load balancing mechanism was being used by the cluster head of the ETASA algorithm. ETASA algorithm being measured performance parameters like high traffic rate, low energy for selecting cluster head and also dealt redundant data transmission. Majorly redundant data transmissions enhance load balancing and energy efficiency in heterogeneous-based WSN environments. Additionally, this algorithm also introduced the sleep awake mechanism. Almost ETASA improvised 15% lifetime improvement by means of energy reduction compared to existing convolution algorithms. Yet another work proposed for heterogeneous environment routing and routing algorithm called Layered and heterogeneous clustering routing algorithm (LHC) [41]. The application that utilized this algorithm was the field observation instruments network. LHC was modified from the LEECH algorithm. Based on the initial energy of nodes, this network is classified into normal and advanced nodes. If the initial energy of the node has more energy, then respective a node acts as advance nodes otherwise normal node. In this LHC algorithm Cluster Heads are formed using only advanced nodes. Later to divide the entire network into several layers a hierarchical structure was used and each layer elect cluster heads.

Each round of cluster head selection a mechanism-based distance and energy were considered including residual energy. Later in conducted experiment data transmitted capacity and energy efficiency were measured and compared with the LEACH algorithm. Tab. 3 is listing the few routing algorithms and their adaptation in heterogeneous environment based WSN.

Table 3: Heterogeneous based network's clustering mechanisms

S. no	Clustering name	Mechanism	Performance
1	Multi-level heterogeneous routing	Learning automata for cluster head selection	Stability and lifetime of network
2	ETASA	sleep awake mechanism	high traffic rate, low energy for selecting cluster
3	LHC	into several layers a hierarchical structure	data transmitted capacity and energy efficiency

Additionally, to compare more existing routing algorithms, work related to various routing protocols for WSN was addressed recently [42]. In this work various existing routing algorithms such as SPIN, RR, GBR, CADR, PEGASIS, Self-organizing protocol (SOP), Virtual grid architecture routing (VGA), LEECH, APTEEN, TEEN, GEAR, SAR. It is important to analyze the performance of all routing algorithms along with their unique features. Tab. 4 is listing the routing algorithm along with its working parameter and features.

Table 4: Various routing algorithm and features

S. no	Algorithm	Scalability	Data aggregation	Delivery mechanism	Overhead	Power consumption
1	SPIN	Low	Yes	Event	Less	Less
2	RR	High	Yes	Demand	Less	Less
3	GBR	Low	Yes	Hybrid	Less	Less
4	CADR	Low	Yes	Continues	Less	Less
5	PEGASUS	High	No	Chain	Less	More
6	SOP	High	No	Continues	More	Less
7	VGA	High	Yes	Continues	More	Less
8	LEACH	High	Yes	Clustered	More	More
9	HLEACH	High	Yes	Clustered	More	More
10	APTEEN	More	Yes	Threshold	More	More
11	TEEN	More	Yes	Threshold	More	More
12	GEAR	Low	No	Demand	Average	Less
13	SAR	Low	Yes	Continues	More	More
14	LHC	More	Yes	Clustered	Less	Less
15	ETASA	More	Yes	Clustered	Less	Less
16	EEUC	Low	No	Threshold	More	More
17	HCC	Low	No	Threshold	More	More
18	PEACH	Low	No	Threshold	More	More

Even though system models, clustering algorithms and routing algorithms have been introduced in various applications for efficient cluster-based routing, there were no trust-aware mechanisms introduced.

Trust aware and efficient clustering and intrusion system must be adapted in trust aware systems. There is a research gap existing that there is not a combined framework-like structure which incorporates, to reduce energy, provide the shortest path to reach source to destination in the military and other WSN applications and thereby extending the lifetime of the wireless sensor.

3 Problem and Contribution

The main objective of the proposed work is reducing the energy and yield the optimal routing of heterogeneous unmanned vehicle. The proposed hybrid energy optimization of unmanned method consists of four processing steps such as system model, clustering of nodes in heterogeneous environment, trust aware recommendation and routing. The system model used to represent model definition and assumption of unmanned WSN. The clustering is used to find the lifetime nodes and find the energy level of nodes. The fish swarm optimization algorithm (FSO) used for the energy optimization and monitors the energy. The benefits of FSO includes high convergence speed, flexibility, fault tolerance and high accuracy. Using the direct and indirect interaction the trust aware recommendation of nodes is traced and based on the direct and indirect tracing the life of the nodes is calculated. The based on the loop free routing protocols mobile nodes and behavior of the mobile nodes are traced and Finally, the hybrid algorithm are presented.

3.1 System Model

The system model described in the Fig. 1. The system model connected using base stations (BS), unmanned vehicle with sensor and devices, various connecting nodes with cluster and cluster heads. All the components of the system model are well interconnected each other and data transferred to unmanned vehicle and BS. The basic definition of the environments and assumptions of proposed work are as follows.

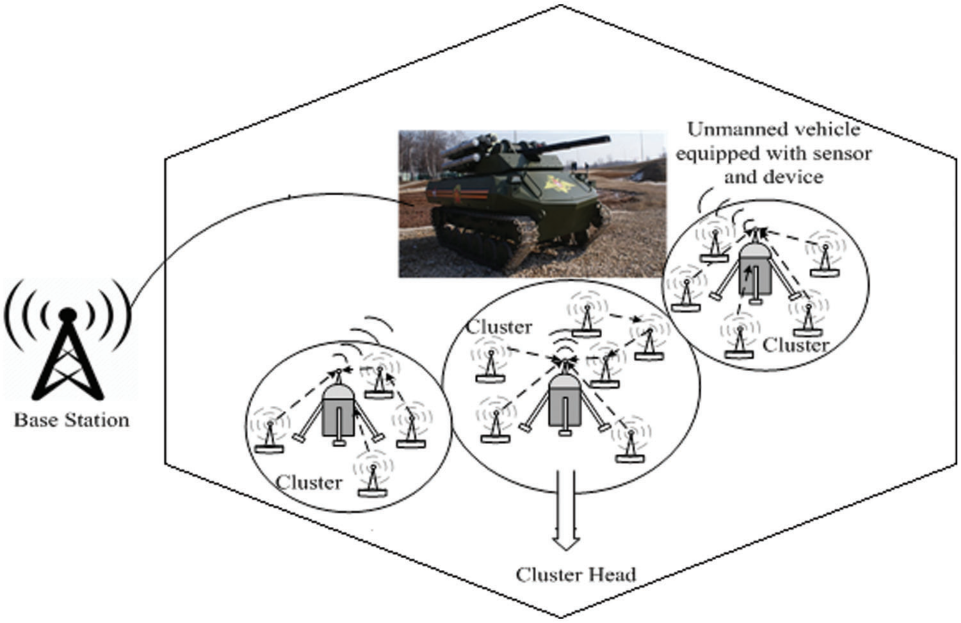

Figure 1: System model and connected devices

3.1.1 Definition

In this work ‘N’ sensors are arrayed in the heterogeneous environments with the distance ‘D’ and radius ‘R’. The connected sensors are represented as $\{N_1, N_2, \ldots, N_n\}$. The connected sensors are move freely in the heterogenous fields. The connected sensors are clustered as per the several sectors and each sensor are clustered as per the positions, distance ‘D’ and radius ‘R’.

3.1.2 Assumptions

i) All the heterogeneous environments sensors of unmanned vehicles are interconnected.
ii) All the sensors have unique ID, location knowledge, energy levels and information interchange details.
iii) The movements of the sensor nodes are well scheduled and it having transmission direction and distance ranges.
iv) The energy level should be automatically adjusted and self-balanced based on the distance and timing of nodes.

The primary goal of proposed methodology is to optimize the energy and detection of location among the ‘N’ sensor nodes and transmit the information to BS. This proposed work is applied in military application for implementations. To detect the location and intruded node, the proposed hybrid method used. The proposed work initially formulates the cluster based on Artificial Fish Swarm Optimization (AFSO) algorithm. The clustered and recommended nodes are evaluated based on the trust recommendation system. And finally, self-starting and network behaviour monitoring routing algorithms are used for routing the nodes (AODV). The proposed methodology represented in the Fig. 2.

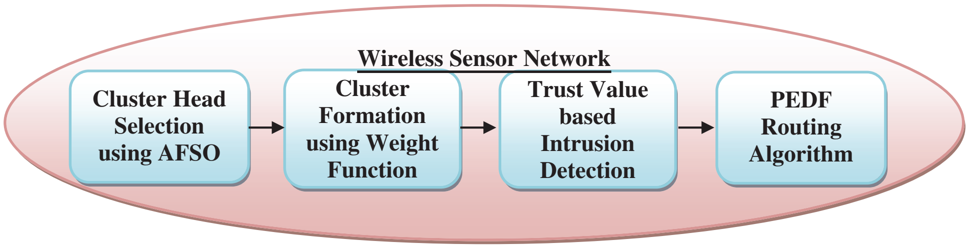
Wireless Sensor Network
Cluster Head Selection using AFSO
Cluster Formation using Weight Function
Trust Value based Intrusion Detection
PEDF Routing Algorithm

Figure 2: Block diagram of proposed work

3.2 Cluster Formation

Initially, the sensors are deployed in grid model in large heterogeneous environments. The life time of the network expand, decrease the power consumption. The proposed cluster formation consists of two stages namely such as cluster head (CH) selection and cluster formation. The CH selection, AFSO algorithm is utilized and clusters are formulated based on the weight.

3.2.1 Cluster Head Selection Process

The CH selection process, performed using AFSO algorithm. By using CH selection process, improve the life span of the network and reduce the failure node. The proposed AFSO algorithm was introduced by Li in 2002 and depends on the behavior of the fish swarm. The natural fish swarm is looking for a food source to hunt, as well as this method of obtaining a global optimal solution. Each artificial fish in AFSA follows four behaviours or operations such as searching operation, swarming operation, following operation and arbitrary operation to get the optimal solution. To solve the problem lot of meta-heuristic algorithms are utilized namely, Genetic Algorithm (GA), Partical Swarm Optimization (PSO), Finite Automata (FA), Cuckoo Search (CS) algorithm, Gravitational Search Algorithm (GSA), Group Search Optimizer (GSO) and

AFSO etc. Higher accumulation speed, flexibility, fault tolerance and high accuracy is due, AFSO used for instruction. The procedure of step-by-step cluster head selection process is presented as follows.

Step 1: Chaotic based solution initialization: Initially, the parameter used in AFSO and number of sensor nodes is inserted. Artificial fish or plugged with N the population size and locations of the applicant solutions. The calculation of the applicant to be selected as the solution or artificial fish is the home of CH.

Initially, chaotic variable is generated with the help of tent map. The tent map can be written as follows;

$$S_{n+1} = \mu\left(1 - 2\left|S_n - 0.5\right|\right),\quad 0 \le S_0 \le 1, \qquad n = 0,\ 1,\ 2,\ \ldots, \tag{1}$$

where, $\mu \in (0,\ 1)$ → Purification parameter.

Using the tent map ($\mu = 1$) we can rewrite the Eq. (2) as follows;

$$S_j^{(i+1)} = \mu\left(1 - 2\left|S_j^{(i)} - 0.5\right|\right),\quad j = 0,\ 1,\ 2,\ \ldots,\ D \tag{2}$$

where, $S_j \rightarrow j^{th}$ Chaos variable, $i \rightarrow$ Chaos iterations, Set $i = 0$ and generate D chaos variables by (3). Then, i = 1, 2… N in turn and initial swarm are generated. Then the chaos variable above $S_j^{(i)}, i = 1, 2, \ldots, N$ will be mapped into the search range of the decision variable:

$$F_{ij} = F_{\min,j} + S_j^{(i)}\ \left(F_{\max,j} - F_{\min,j}\right),\ j = 1,\ 2,\ \ldots,\ D. \tag{3}$$

$$F_i = \left[F_1(t),\ F_2(t),\ \ldots,\ F_i(t)\right] \tag{4}$$

where, $F_i(t)$→Position of the $i^{\ th}$ fish or CHs

Step 2: Fitness or food concentration: After the installation of artificial fishes or solutions, the health of artificial fishes is determined. This exercise is evaluated on the basis of two objective functions. Objective function 1 (O_1) is designed based on Average distance (AD) and objective function 2 is designed based on Residual Energy (RE).

Objective function 1:

The average distance is considered as an objective function 1 (O_1). Average distance is calculated between CH and SNs. The average system should be minimized. The average distance is can be calculated as follows;

$$Min\,(O_i) = \sum_{i=1}^{n} \frac{1}{m}\left(\sum_{j=1}^{m} d(SN_j,\ CH_i) + d(CH_i,\ BS)\right) \tag{5}$$

where, m–Amount of SNs in the sensing area, n –Number of CHs to be chosen, $SN_j,\ CH_i$-Normal separation among CH and rest of the SNs in the intra-cluster, $CH_i,\ BS$→Average distance between a BS and CH.

Objective function 2:

The residual energy is considered as the objective function 2 (O_2). The absolute remaining energy of all CHs ought to be expanded for electing the optimal CH. The objective function 2 can be calculated as follows;

$$\min\,(o_2) = \frac{1}{\sum_{i=1}^{n} Energy_{CH_i}} \tag{6}$$

where, $Energy_{CH_i}$→ Total residual energy of all CH_i

Using Eq. (1) the fitness of each artificial fish is calculated.

$$Fit_i(t) = O_1 \times \beta + O_2 \times (1 - \beta), \quad 0 < \beta < 1 \tag{7}$$

A fish with minimum fitness value has best location, i.e., the best is the cluster head selection.

***Updation*:** After calculating the fitness of each fish, we update the position of artificial fish using AFSO. Each artificial fish in AFSA follows four behaviours or operations such as searching operation, swarming operation, following operation and irregular operation to obtain the optimal solution.

***Searching operation*:** At first, the present situation of an artificial fish is represented as Y_i and it picks a j^{th} position Y_j that display is an arbitrary distance. The fitness of both Y_i and Y_j are paralleled. If the fitness of Y_j is better than that of Y_i, at that point it ahead of a *Step* to the heading of $(Y_j - Y_i)$. Otherwise, the random operation will be initiated. In irregular activity, the artificial fish picks next position Y_j determines whether or not the selected position completes the moving position. The random operation proceeds if the touching complaint isn't satisfied by the picked location. The standard for looking through operation is determined as follows:

$$\tilde{Y}_i = \begin{cases} Y_i + Step * \dfrac{Y_j - Y_i}{D_{ij}} * rand, & if \; Fit_j < Fit_i \\ Random \; operation, & otherwise \end{cases} \tag{8}$$

where, $\tilde{Y}_i$→ New position of the artificial fish, Rand→ random number in the range [0, 1],

D_{ij}→ Distance between Y_i and Y_j

***Swarming operation*:** Individual artificial fish Y_i in the swarm investigates the focal location Y_c of the m_f amount of artificial fish in its pictorial separation. The artificial fish Y_i moves to the focal location Y_c if(Fit_c/m_f) is better than $(\delta * Fit_i)$. Otherwise searching operation is initiated. The rule for swarming operation is determined as follows:

$$\tilde{Y}_i = \begin{cases} Y_i + Step * \dfrac{Y_c - Y_i}{D_{ic}} * rand, & if \; (Fit_c/m_f) < (\delta * Fit_i) \\ Searching \; operation, & otherwise \end{cases} \tag{9}$$

where, δ represents the crowd factor in the range [0, 1].

***Following operation*:** In this operation or behavior, the artificial fish Y_i picks the neighborhood best solution or position denoted as Y_{best}. It is moving forward a stage toward the direction $(Y_{best} - Y_i)$ if (Fit_{best}/m_f) is better than $(\delta * Fit_i)$. Otherwise, the searching operation is initiated. The rule for the following operation is determined as follows:

$$\tilde{Y}_i = \begin{cases} Y_i + Step * \dfrac{Y_{best} - Y_i}{D_{i,\,best}} * rand, & if \; (Fit_{best}/m_f) < (\delta * Fit_i) \\ Searching \; operation, & otherwise \end{cases} \tag{10}$$

Random operation: In this operation, a position is chosen randomly by the artificial fish. If the fitness of the chose position is better than that of the current situation of the artificial fish, at that point it shifts the chose position. This operation is random operation.

Termination: The above activities have been followed up to find the optimal solution. Once the best possible CH is obtained, then the algorithm will be done. This optimal CH is utilized for cluster formation.

Algorithm 1: Optimized CH using AFSO

```
Input: Candidate solutions, $Step$, $m_f$, $rand$, $\delta$ and $Visual$
Output: Optimal CH
    1. Initialize the situation of artificial fishes or solutions utilizing Eqs. (1)–(4)
    2. Determine qualification for utilizing Eq. (7).
    Searching operation:
    3. If the $Fit_j < Fit_i$
    4. Formerly
       $\tilde{Y}_i = Y_i + Step * \frac{Y_j - Y_i}{D_{ij}} * rand$
    5. Else
       The random operation is initiated
    6. End
    Swarming operation:
    7. If $(Fit_c / m_f) < (\delta * Fit_i)$
    8. Then
       $\tilde{Y}_i = Y_i + Step * \frac{Y_c - Y_i}{D_{ic}} * rand$
    9. Else
             Searching operation is initiated.
    10. End
    Following Operation:
    11. If $(Fit_{best} / m_f) < (\delta * Fit_i)$
    12. Then
        $\tilde{Y}_i = Y_i + Step * \frac{Y_{best} - Y_i}{D_{i,best}} * rand$
    13. Else
           Searching operation is initiated
    14. End
    Random operation:
    15. Random solution $Y_{random}$ is selected.
    16. If $Fit_{random} < Fit_i$ $\tilde{Y}_i = Y_{random}$
        Else
        $\tilde{Y}_i = Y_i$
    17. End
    18. Steps 2–19 are preceded until finding the optimal solution or Optimized FIS system.
    19. This optimized FIS system is used as the CAC decision maker.
```

B. Cluster formation

After the CH selection process, clusters are formed based on the weight function. The wight function can be calculated using Eq. (11).

$$W(SN_j,\ CH_i) = \alpha \frac{R_E(CH_i)}{d(SN_j,\ CH_i) \times d(CH_i,\ BS)} \tag{11}$$

where, $R_E(CH_i)$→ Residual energy of CH, $\frac{1}{d(SN_j,\ CH_i)}$→ Reciprocal of distance between $\mathrm{SN_j}$ and $\mathrm{CH_{i,}}$ $\frac{1}{d(CH_i,\ BS)}$ →Equal of separation among CH and BS, α→ Constant value.

Using Eq. (11), the weight of each SN is determined. In light of the weight value the clusters are formulated.

3.3 Trust Aware Value Recommendation System

The trust aware value recommendation system used to select the node based on the life time of nodes. The trust aware recommendation is performed using direct and indirect interaction. After cluster formulation, each cluster the intruded node is selected with the help of trust value. The intruded nodes are easy to fail and if any node fails during the transmission period, the total information are loosed and life time of the system also reduced. To overcome the problem, before routing, the intruded nodes are identified. The total trust value of every hub is determined dependent on the immediate and backhanded trust value.

The trust value is determined in two way namely, direct and indirect interaction. Let, node j forward the packet to a node i means, the direct trust (T_{direct}) can be calculated as follows;

$$T_{direct} = \frac{F_{i,j}(t)}{R_{i,j}(t)} \tag{12}$$

where; $F_{i,j}(t)$→Number of packets forwarded by node$i$ at time t, $R_{i,j}(t)$→Number of packets productively established by node n from node m at time t, If node j has N number of neighbors, $T_{indirect}$ can be calculated as

$$T_{indirect} = \frac{1}{N}\sum_{k=1}^{N} T_{neighbors}(t) \tag{13}$$

$T_{indirect}$ is the normal of the accessible trust degrees of the neighbors at time t. The total trust value is calculated using Eq. (14)

$$T_{total} = \omega_1\ T_{direct} + \omega_2\ T_{indirect} \tag{14}$$

ω_1 and ω_2 are characterize the weight factors of T_{direct} and $T_{indirect}$ correspondingly. These weight factors can be determined as

$$\omega = \begin{cases} 1, & No.\,of\ untrust\ nodes = 0 \\ \dfrac{No.\,of\ trust\ nodes}{No.\,of\ untrust\ nodes}, & otherwise \end{cases} \tag{15}$$

If the T_{total} of a node is maximum the $T_{threshold}$, that node with high lingering energy is chosen as a CH to the cluster. If the T_{total} is minimum the $T_{threshold}$, then the node should be avoided as a dangerous node. The node detection algorithm shown in the Algorithm 2.

Algorithm 2: Trust node detection

```
1. Initialize $i^{th}$ nodes in a cluster.
2. For $i$
        $Calculate\ T_{direct}, T_{indirect}\ and\ T_{total}$
3. If   $T_{total} > T_{threshold}$
$i = Trusted\ node$
Else
Next $i$
```

3.4 Routing Algorithms

After effective node detection, the Routing is performed in the heterogeneous environments. The routing is performed based on the CH. Here, the sensor node sends the sensing information to CH. Initially, the CH check the node based on the trust value. If the node is normal node means the CH send the data to nearest BS. Otherwise, CH omits the data. The proposed method used self-starting, network behaviour monitoring and geo positioning based propriety routing algorithm. The comparison of the various protocol is presented in the Tab. 3.

The proposed method used Priority Energy based Data Forwarding algorithm (PEDF) [43], which is choose the suitable path based on the energy level, maximize the throughput and minimize the delay. The priority important of PEDF shown in the Tab. 5.

Table 5: Priority Level of PEDF

Importance	Priority level
Urgent	Priority 1
Highly	Priority 2
Moderate	Priority 3
Less Important	Priority 4

The main advantages of PEDF algorithm is continuously report the energy level in multiple path and choose the best optimal paths dynamically in the heterogeneous environments. Similarly, the PEDF is record all the geographical location of each node dynamically. So, the behavior of nodes and position of the node monitored by the central clustered head. The optimized, sample node path for multiple transmissions between sources (S) to destination (D) are shown in Fig. 3. The transmission path between source to destination has chooses from multiple paths and select the best three paths from the multiple paths. The best selected path based on the maximum throughput, energy level and traffic etc.

4 Simulation and Discussion

The proposed intrusion detection in WSN experimental results is analysed in this section. For simulation of the proposed work has been done with the help of Network Simulator version-2 tool. The proposed simulation parameters are given in Tab. 6. The main objective of proposed methodology is to select the optimal CH with the help of AFSO. Then, the intruded nodes are calculated using trust values recommendation system. The achievement of proposed methodology is analysed in terms of different metrics. The proposed method stimulated in the military application environment. The fundamental function of the WSN with enemy minutes and co-organizing exercises of the army shown in Fig. 4. The IoT sensors are used to monitor the environments and routing algorithm used to find the geographical positions. The various sensors send the surrounding information to BS. The base station controls all the devices and manage the positions of each node. The entire simulation environment of proposed work military application shown in Fig. 4.

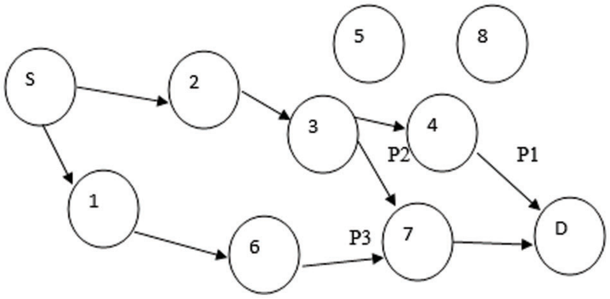

Figure 3: Multiple transmission path

Table 6: Simulation parameters

Parameter name	Value
Number of nodes	400
Wireless protocol	802.11
Area	1000 × 1000
Simulation time	50 s
Packet size	512
Transmit power	0.660 W
Receiving power	0.395 W
Initial energy	40 J
Transmission range	250 m
Constant bit rate	500 kbps

In Fig. 4, sensors are deployed between unmanned districts of a huge military barrack. The soldiers are monitor the military barrack in the border position. In this manner, monitor entire military barrack and deployed "*n*" number of sensors in the large military barrack. The sensors are placed in the region using two models namely, random model and grid model. In this work, we deployed the sensors in random and heterogeneous model.

4.1 Evaluation Metrics

The performance of the system is measured based on the standard statistical measures such as Delay, Delivery ratio, energy, throughput and NLT. The results are investigated with the existing techniques as far as different standard assessment measurements to demonstrate the system effectiveness.

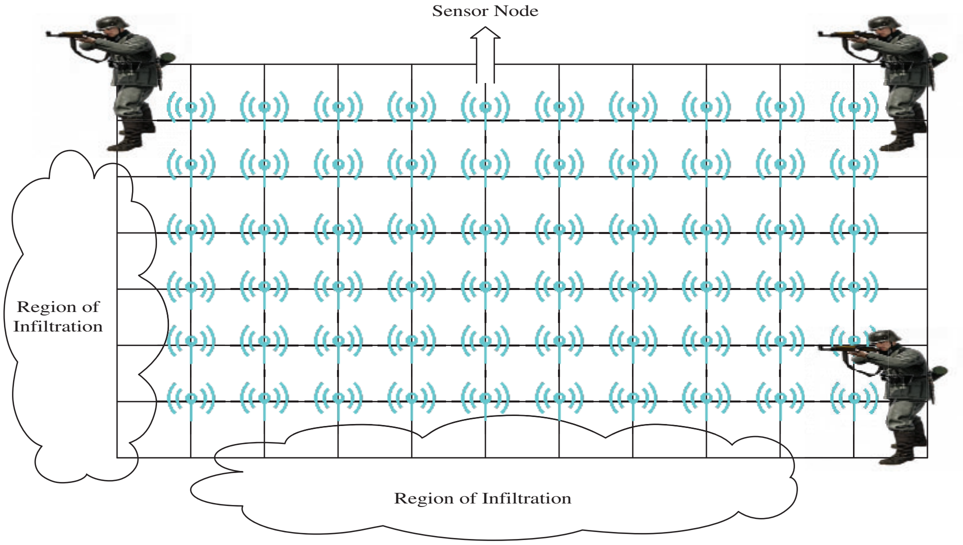

Figure 4: WSN based military monitoring system

Delay time: The normal time it takes an information packet to arrive at the goal. This fuses each conceivable deferral brought about by buffering during course discovery latency, lining at the interface queue. This is the time of the measurement target key data packet from the source is determined by subtracting the time of the essential pocket transmitted.

Delivery Ratio: Packet delivery ratio is the ratio that is utilized to ascertain the quantity of an information packet transmitted by the source hub and no. of information gotten by the goal hub. It is utilized to compute the loss rate of information packets while during information transmission in the simulation network. It assesses the loss rate and measures up both the rightness and proficiency of ad-hoc routing conventions. A higher packet conveyance ratio is trusted in any system.

$$Packet\ Delivery\ Ratio = \sum Number\ of\ packet\ received / \sum Number\ of\ packet\ send$$

Throughput: Throughput can be characterized as what number of information packets gotten by the receiver within information transmission time or successful information transmission performed within a time period. In any system, throughput is the average rate of effectively information packet conveyed from source hub to goal hub. Throughput is represented in bits/bytes every second. In any system higher throughput is the most basic factor.

$$Throughput = \sum Number\ of\ successful\ packet\ transfered / Unit\ time$$

4.2 Performance Comparison

The simulated outcome displays the performance assessment of both the projected and existed protocol. The cluster formation of the proposed work shown in the Fig. 5. The proposed work is compared with two existing algorithms such as genetic algorithm (GA) and fission -fusion (FF) [44] selection using genetic algorithm. The simulation work of proposed method compared with help of various Evaluation metrics.

The Tab. 7 shows the performance comparision of the genetic algorithm(GA), fission-fusion (FF) and proposed AFSO algorithm. The results shows proposed AFSO algorithm performs better than the existing algorithms. Hence the proposed algorithm is validated.

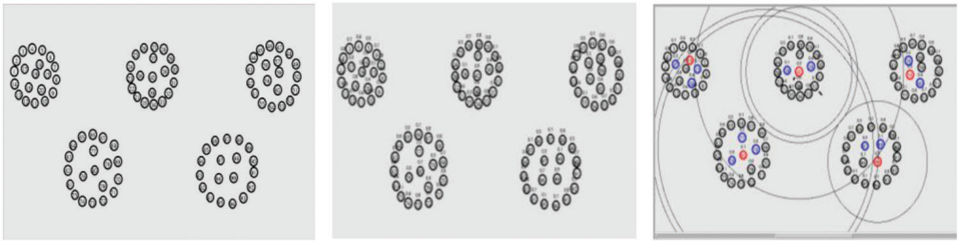

Figure 5: Procedure of cluster formation

Table 7: Performance comparision of various optimization techniques

Nodes	Delay *10^3			Delivery ratio			Throughput			Energy			Network Life Time		
	GA	FF	AFSO	GA	FF	AFSO	GA	FF	AFSO	GA	FF	AFSO	GA	FF	AFSO
100	0.4	0.2	**0.9**	50	24	**100**	23	16	**78**	50	100	**0**	0	8	**9**
200	1	0.8	**0.2**	100	45	**200**	10	9	**95**	150	200	**0**	0	3	**4**
300	2.2	2	**0.2**	150	55	**300**	8	7	**96**	250	300	**0**	0	2	**3**
400	2	1.8	**0.92**	200	75	**400**	7	6	**96**	350	400	**0**	0	1	**2**

In Fig. 6, the packet drop rate of the routing convention is portrayed. Along these lines, the diagram demonstrates that the proposed strategy has less delay when contrasted and the current convention in terms of network flow. Fig. 7, demonstrates the flow of hubs in the routing convention. At the point when contrasted with the existing strategy the proposed technique gives high effectiveness in conveying the packet. The diagram obviously demonstrates the precision level in delivering the packet contrasted with the existing one, which is calculated using the packet delivery ratio formula mentioned in 4.1.

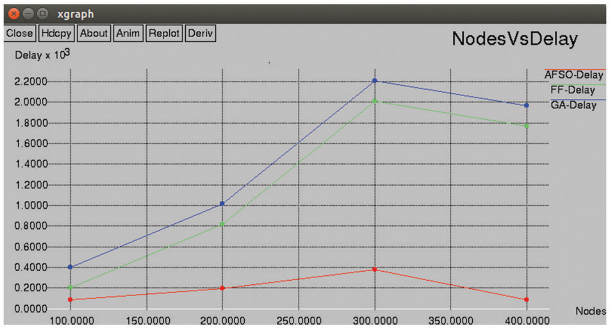

Figure 6: Nodes *vs.* delay

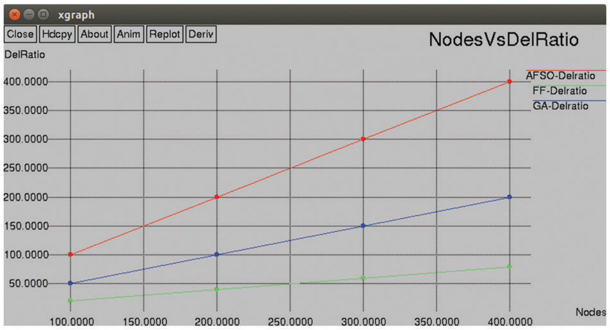

Figure 7: Node *vs.* delivery ratio

Fig. 8, shows the result of throughput obtained for proposed AFSO and existing FF and GA techniques by varying the nodes. The proposed AFSO algorithm acheives the efficient outcome than other algorithms. Figs. 9 and 10 shown the performance metrics of proposed AFSO algorithm achieves the efficient outcome than other existing techniques like FF and GA by varying the nodes.

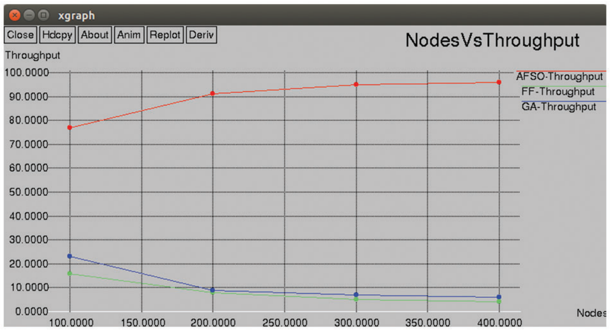

Figure 8: Node *vs.* throughput

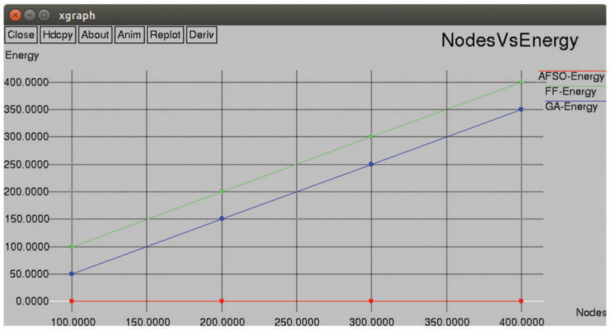

Figure 9: Node *vs.* energy

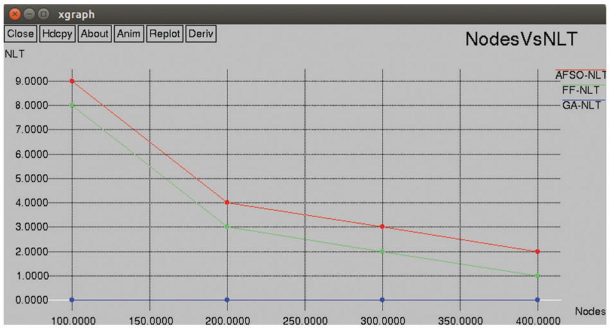

Figure 10: Node *vs.* network life time (NLT**)**

5 Conclusion and Future Enhancement

In this proposed work, an energy efficient Trust aware optimal method had proposed for WSN. The proposed system consists of clustering using optimization, trust aware recommendation and routing. First, the cluster formation is done by the Artificial Fish Swarm Optimization (AFSO) algorithm, which provides stable efficient cluster formation. After the cluster head selection, cluster region is formed.

Second the trust aware value recommendation system used to select the node based on the life time of nodes. Third, the priority-based routing algorithm is used in route the sensing nodes. This hybrid recommendation system is reducing the energy in heterogeneous environments and applied in the military application. The outcome of the proposed work helps to avoid energy loss and reduce the failure nodes. The simulation of the proposed work is simulated using NS platform. The predicted results are compared with previous work and metrics results are produced best results in delay, delivery ratio, energy and throughput. This work is enhanced in different directions movements of sensors and searching the multipath in heterogeneous environments. The proposed approach can be analyzed and evaluated based on sink node. The suggested, sink node can be approached to a set of low energy nodes to reduce energy consumption. It can also be extended efficiently based on AI based clustering techniques and advanced IoT components.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflict of interest to report regarding the present study.

References

[1] A. Bleda, F. Fernandez-Luque, A. Rosa, J. Zapata and R. Maestre, “Smart sensory furniture based on WSN for ambient assisted living,” *IEEE Sensors Journal*, vol. 17, no. 17, pp. 5626–5636, 2017.

[2] J. Wu, K. Ota, M. Dong and C. Li, “A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities,” *IEEE Access*, vol. 4, pp. 416–424, 2016.

[3] S. Jokhio, I. Jokhio and A. Kemp, “Light-weight framework for security-sensitive wireless sensor networks applications,” *IET Wireless Sensor Systems*, vol. 3, no. 4, pp. 298–306, 2013.

[4] F. Valeur, G. Vigna, C. Kruegel and R. Kemmerer, “Comprehensive approach to intrusion detection alert correlation,” *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 3, pp. 146–169, 2004.

[5] A. Mishra, K. Nadkarni and A. Patcha, “Intrusion detection in wireless adhoc networks,” *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48–60, 2004.

[6] N. Ye, Q. Chen and C. Borror, “EWMA forecast of normal system activity for computer intrusion detection,” *IEEE Transactions on Reliability*, vol. 53, no. 4, pp. 557–566, 2004.

[7] R. Erbacher, K. Walker and D. Frincke, “Intrusion and misuse detection in large-scale systems,” *IEEE Computer Graphics and Applications*, vol. 22, no. 1, pp. 38–47, 2002.

[8] B. Hoyle, M. Rau, K. Paech, C. Bonnett, S. Seitz *et al.,* “Anomaly detection for machine learning redshifts applied to SDSS galaxies,” *Monthly Notices of the Royal Astronomical Society*, vol. 452, no. 4, pp. 4183–4194, 2015.

[9] B. Sun, L. Osborne, Y. Xiao and S. Guizani, “Intrusion detection techniques in mobile adhoc and wireless sensor networks,” *IEEE Wireless Communications*, vol. 14, no. 5, pp. 56–63, 2007.

[10] Y. Wang, X. Wang, B. Xie, D. Wang and D. P. Agrawal, “Intrusion detection in homogeneous and heterogeneous wireless sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698–711, 2008.

[11] S. Shin, T. Kwon, G. Jo, Y. Park and H. Rhy, “An experimental study of hierarchical intrusion detection for wireless industrial sensor networks,” *IEEE Transactions on Industrial Informatics*, vol. 6, no. 4, pp. 744–757, 2010.

[12] S. Bu, F. Yu, X. Liu and H. Tang, “Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 3064–3073, 2011.

[13] F. Bao, I. Chen, M. Chang and J. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[14] M. Wei and K. Kim, “Intrusion detection scheme using traffic prediction for wireless industrial networks,” *Journal of Communications and Networks*, vol. 14, no. 3, pp. 310–318, 2012.

[15] J. Chen, J. Li and T. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors: Global and local," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4742–4755, 2013.

[16] A. Abduvaliyev, A. K. Pathan, J. Zhou, R. Roman and W. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[17] B. Sun, X. Shan, K. Wu and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 13–25, 2013.

[18] V. Matyas and J. Kur, "Conflicts between intrusion detection and privacy mechanisms for wireless sensor networks," *IEEE Security & Privacy*, vol. 11, no. 5, pp. 73–76, 2013.

[19] G. Han, J. Rodrigues, J. Jiang, L. Shu and W. Shen, "IDSEP: A novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *IET Information Security*, vol. 7, no. 2, pp. 97–105, 2013.

[20] H. Moosavi and F. Bui, "A Game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1367–1379, 2014.

[21] G. Han, X. Li, J. Jiang, L. Shu and J. Lloret, "Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks," *the Computer Journal*, vol. 58, no. 6, pp. 1280–1292, 2014.

[22] J. Duan, D. Gao, D. Yang, C. H. Foh and H. H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[23] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb and A. W. Khan, "TERP: A trust and energy aware routing protocol for wireless sensor network," *IEEE Sensors Journal*, vol. 15, no. 12, pp. 6962–6972, 2015.

[24] K. Huang, Q. Zhang, C. Zhou, N. Xiong and Y. Qin, "An efficient intrusion detection approach for visual sensor networks based on traffic pattern learning," *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 47, no. 10, pp. 2704–2713, 2017.

[25] Z. Zhang, H. Zhu, S. Luo, Y. Xin and X. Liu, "Intrusion detection based on state context and hierarchical trust in wireless sensor networks," *IEEE Access*, vol. 5, pp. 12088–12102, 2017.

[26] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb and A. W. Khan, "A trust aware routing protocol for energy constrained wireless sensor network," *Telecommunication Systems*, vol. 61, no. 1, pp. 123–140, 2016.

[27] H. Sedjelmaci, S. Senouci and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in uav-aided networks: A Bayesian game-theoretic methodology," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1143–1153, 2017.

[28] G. Rajeshkumar and K. R. Valluvan, "An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network," *Wireless Personal Communications*, vol. 94, no. 4, pp. 1993–2007, 2017.

[29] D. Santoro, G. Escudero-Andreu, K. Kyriakopoulos, F. Aparicio-Navarro, D. Parish *et al.,* "A hybrid intrusion detection system for virtual jamming attacks on wireless networks," *Measurement*, vol. 109, pp. 79–87, 2017.

[30] N. Alsaedi, F. Hashim, A. Sali and F. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)," *Computer Communications*, vol. 110, pp. 75–82, 2017.

[31] G. Y. Keung, B. Li and Q. Zhang, "The intrusion detection in mobile sensor network," in *Proc. of ACM MobiHoc*, Chicago, USA, pp. 11–20, 2010.

[32] H. Hu, Y. Huang, X. Da, H. Zhang, W. Gao *et al.,* "Optimization of energy utilization in cognitive UAV systems," *IEEE Sensors Journal*, vol. 21, no. 3, pp. 3933–3943, 2021.

[33] Z. Sun, Y. Xu, G. Liang and Z. Zhou, "An intrusion detection model for wireless sensor networks with an improved v-detector algorithm," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 1971–1984, 2018.

[34] S. Redhu and R. M. Hegde, "Cooperative network model for joint mobile sink scheduling and dynamic buffer management using q-learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1853–1864, 2020.

[35] S. Ghosh, S. De, S. Chatterjee and M. Portmann, "Learning-based adaptive sensor selection framework for multi-sensing WSN," *IEEE Sensors Journal*, vol. 99, pp. 1, 2021.

[36] N. Shabbir and S. R. Hassan, “Routing protocols for wireless sensor networks (WSNs)”, in *Wireless Sensor Networks - Insights and Innovations.* London, *United Kingdom: IntechOpen*, 2017.

[37] E. Pei, J. Pei, S. Liu, W. Cheng, Y. Li *et al.,* “A heterogeneous nodes-based low energy adaptive clustering hierarchy in cognitive radio sensor network,” *IEEE Access*, vol. 7, pp. 132010–132026, 2019.

[38] J. Huo, J. Yang and H. M. M. Al-Neshmi, “Design of layered and heterogeneous network routing algorithm for field observation instruments,” *IEEE Access*, vol. 8, pp. 135866–135882, 2020.

[39] H. El Alami and A. Najid, “ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks,” *IEEE Access*, vol. 7, pp. 107142–107153, 2019.

[40] S. Tanwar, S. Tyagi, N. Kumar and M. S. Obaidat, “LA-MHR: Learning automata based multilevel heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of WSN,” *IEEE Systems Journal*, vol. 13, no. 1, pp. 313–323, 2019.

[41] M. Adimoolam, M. Sugumaran and R. S. Rajesh, “A novel efficient clustering and secure data transmission model for spatiotemporal data in WSN,” *International Journal of Pure and Applied Mathematics*, vol. 118, no. 8, pp. 117–125, 2018.

[42] N. M. Shagari, M. Y. I. Idris, R. B. Salleh, I. Ahmedy, G. Murtaza *et al.,* “Heterogeneous energy and traffic aware sleep-awake cluster-based routing protocol for wireless sensor network,” *IEEE Access*, vol. 8, pp. 12232–12252, 2020.

[43] V. Deepali, T. Dhruv, D. Arun and B. Tushar, “Priority based energy-efficient data forwarding algorithm in wireless sensor networks,” arXiv e-prints: 1305.2369, 2013.

[44] A. K. Das and D. K. Pratihar, “A Fission-fusion (FF) selection scheme for genetic algorithms,” *IEEE Region 10 Symposium (TENSYMP)*, pp. 277–281, 2019.