International Journal of Modern Agriculture, Vol. No10, Issue No. 2(2021)
ISSN: 2305-7246

Secure Communication in Wireless Sensor Network Using Intrusion Detection System for Agriculture

[1]O.P.Uma Maheswari , [2]Dr.S.Jayasankari ,

[1]Research Scholar,Department of Computer Science, P.K.R. Arts College For Women, Gobichettipalayam.
[2]Associate Professor, Department of Computer Science, P.K.R. Arts College for Women, Gobichettipalayam,

Abstract

Recent advancement in Wireless Sensor Network (WSN) affords lot of sophistication in people's day to day life which in turn increases its demand. WSN find its applications in various fields such as prediction of natural disaster, environmental monitoring, home appliances encompassing various areas like agriculture, and health care, clustered databases and so on. Path Finding Agent (PFA) is an eminent approach exploited for sensor nodes transmission of stored information to the cluster heads in case of agriculture information communication. The secured mechanism should be significantly utilized to prevent against such as node capture, physical tampering, eavesdropping, denial of service, etc. due to the deployment of WSN in remote places which are left unattended. The prevailing researches concentrate only on energy proficiency rather than security which in turn causes information loss and may transmit false information to the to the target. A hybrid optimization is chiefly involved to mitigate this issue for choosing cluster head which in turn diminishes the energy consumption. Besides intrusion detection system is also utilized for key generation involving cryptographic method for data encryption and substantiation for circumventing all sorts of attacks with improved security through RSA technique. Path Finding Agent (PFA) and key authentication has its own role in transmission of encrypted information to the cluster heads through the sensor nodes. Query Agent (QA) supports in aggregating the information received by the sensor nodes in the field through cluster head before transporting to the sink node and as a final point decryption of data is achieved through same key. The Proposed approach is validated through experimental results expending USGS databases pertaining to improved security, packet delivery ratio, Network lifetime,throughput and minimized energy consumption.

Keywords: *Cluster head selection, Energy consumption, Agriculture information, Path Finding Agent, Hybrid optimization, Key generation, RSA Cryptography.*

1. INTRODUCTION

The nodes that densely dispersed have assisted in Signal Processing, Sensing, Embedded Computing, and Connectivity in a Wireless Sensor network. In various unique patterns, the sensors were arranged, which possibly be a short-hop, multi-hop, or a point to point master-slave combination. The design methodologies are needed across a set of disciplines including information processing, network as well as operational management, confidentiality, integrity, availability and in network or local processing. The most significant, and essential element of WSN is the sensor node that has the capability to accumulate, and process the associated data, besides it interacts with other member nodes of the network [1] [2].

In order to produce high yielding food crops and to reduce the struggles of the farmers through WSNs, agriculture is one of the most desirable and potential provisions, thus the Precision agriculture (PA) has presented with a number of research works. Generally, PA tend to prohibit the repetition of a certain crop management routine for the crops without considering the site scenarios as well as to enhance the field

management on many aspects. PA provides better pesticide usage management which eventually reduces the wastage resulting in better administration of pests, weeds, diseases and also it ensures that necessary nutrients were given to the crops and thus it turns out to be a dominant high yielding, green agriculture [3] [4].

To communicate the agriculture information, the WSN technology has employed in the current study, where the transmission of the saved data has initiated towards the cluster heads by the sensor nodes using Path Finding Agent (PFA). Most of the time, these networks have installed and abandoned in remote regions. This may result in physical tampering, eavesdropping, node capture, denial of service and many more and these are the reasons that security frameworks are necessary to be safeguarded [5][6]. Inspite of these facts, the current study solely concentres the energy efficiency not on security which may result in data missing and transference of false information towards destination [7].

To confront this challenge, through Hybrid optimization the cluster heads have chosen as regards the reduction of Energy consumption. In terms of evading various possible attacks, an intrusion detection system has presented in this study, where a RSA cryptographic technique takes place to generate the key for encrypting and authenticating the information. Ultimately, the PFA and key authentication process enable the sensor nodes to initiate the transmission of encrypted data to the cluster heads. Pre-transmission of the field driven data obtained by the sensor nodes to the sink nodes using Query Agent (QA), the Cluster heads accumulate them, subsequently the data has decrypted through the same key. [8][9][10].

2. Related works

Ali et al [11] tend to monitor the agriculture, for which they outlined an innovative remote user authentication strategy with the help of WSN. The Burrows–Abadi–Needham (BAN) logic verifies the protocol, besides Automated Validation Information Security Protocols and Applications (AVISPA) tool simulates it. Furthermore, the Random Oracle Design has involved to help in the formal assessment of the system security. Moreover, the fact that the safety of the proposed approach, and its ability to resist the harmful attacks is evident through the informal security assessment, which enables the recommended model to implement with ease in a real-life applications.

Sahitya et al [12] introduced a wireless sensor network that exclusively focuses on smart agriculture, which takes the environment into consideration to obtain a genuine input by having Arduino as the fundamental element. In this model, every node contains a cluster of sensors linked to the Arduino and Zigbee (Xbee). Those sensors estimate the values and then send it to Zigbee (Co-ordinator), a centralized device. Post-reception of the values, the experts made an explicit conclusion

Liu, et al [13] proposed a novel approach to deploy WSN with the help of genetic algorithm (GA). In accordance with the following standards to deploy the WSN, the fitness function of GA was built: (1) it is mandatory to position the nodes in the respective plots; (2) k-connectivity should present in WSN; (3) there should not be communication silos in WSN; (4) the minimum distance connecting the node and the plot boundary has to be higher than a defined value, otherwise the nodes will be corrupted by the farmland edge effect. On natural farmland, the deployments have tested, whereas on uneven farmland bisected according to the spatial differences of soil nutrients. The outcomes reveal the scenarios of both WSNs, in which overall coverage has provided, communication silos not existed, besides the nodes have mark the least value of their connectivity is equal to k. The validation has done for the deployment for different values of k and transmission distance (d) to the node. Through the outcome, we get to know that, the minimum connectivity of nodes increases and attains the value equal to k, by setting d to 200 m, as k increased from 2 to 4, simultaneously sustaining the minimum connectivity.

Parganiha and Kumar [14] using hybrid coverage mechanism (EEC-HC) to attain energy efficiency, enhanced coverage and high throughput introduced a new energy efficient clustering. With the help of optimum distance to reduce the un-coverage area in sensor field, the minimum clustering cost function and optimum number of sensor nodes, has been determined by the recommended EEC-HC. To find out animal interventions in agricultural fields and provided smart fencing, the EEC-HC mechanism has stands as a better choice.

For choosing the node and safe guarding the data packet for WSNs Mehetre et al [15] has recommended, a reliable and well defended routing scheme using two-stage security mechanism, and dual assurance scheme. On the basis of Active Trust to protect several kinds of attacks, such as black hole attack, and selective forwarding attack, during routing, both the schemes are developed. The reliable path has been identified and the safe routing paths have been provided with the help of trust and Cuckoo search algorithm by this research. The performance framework that has been used by the recommended scheme is Energy. It is evident through the outcomes of the experiments that, the recommended system is capable of giving the assurance to increase the lifespan of the network and the probability of safe routing path in the network.

Wu et al [16] has recommended a hierarchical structure on the basis of chance discovery and usage control (UCON) technologies to enhance the safety measures of WSNs by also considering the low-complexity and high security needs of WSNs into account. The present attacks by advanced persistent threat detection can be tackled by the characteristics of continuous decision and dynamic attributes in UCON. Adding to that an active flexible chance discovery mechanism to identify unknown attacks has been used. An integrated structure has been recommended, to sketch and apply a technique utilising the mechanism explained above, in which low-level attack identification with simple rules has been done in sensors and high-level attack identification with complex rules has been done in sinks and at the base station. To reduce the attack irrespective of low-level or high-level attacks have been identified, the software-defined networking and the network function virtualization technologies have been used. To get an attack data set for assessment a test has been done. Then, to assess the resource demand and attack identification rate, a simulation was developed. The achievability and the potential of the proposed scheme have been proven by the outcome.

Sujihelen and Jayakumar [17] has structured and researched a feature of the ECC into a full pledged IECC protocol for preventing the duplicated nodes from attacking the WSNs and MWSNs. The ultimate goal is to secure an industrial area utilising the IECC mechanism for enhanced remote monitoring, regarding the application. It is evident through the Simulation assessment that the IECC performs well in static WSN and MWSNs over the present baseline protocols.

3. INFERENCES FROM THE EXISTING WORK

An attacker can create every type of threats and attacks on WSN, because it is often installed at the most unfavourable and fragile environments. Moreover apart from the existing identified threats, this paves a way for advanced persistent threats. These are the present unidentified type of attacks in WSNs. Predominantly the present WSN security parts lack volatile properties, so the ongoing attacks with actively modifying characteristics could not be defended by the old security structures and parts. Adding to that, the unidentified strikes are taken as unconventional strikes in classic trespass identification or prevention systems, as it possess unconventional characteristics, which varies from those of traditional attacks. The attack defending systems in the present WSNs is not able to safeguard from the novel attacks which are able to harm the WSNs, they were predominantly made of the training samples of the traditional threats. Hence, it is mandatory to propose an attack prevention scheme, which is able to fortify the WSNs. Because, the advanced constant threats created by the present unidentified attacks can break into WSNsand disturb their routine actions.

4. PROPOSED METHODOLOGY

The recommended model exploiting the Wireless Sensor Network (WSN) is explained in this part. Namely, clustering, cluster head selection through Hybrid cuckoo search and genetic algorithm optimization, key generation for node attestation and defend the attacks and the sensed data will be transmitted through the chosen cluster head by Path Finding Agent (PFA) are the four parts of this model. The recommended work's complete structure has been illustrated in the figure 1.

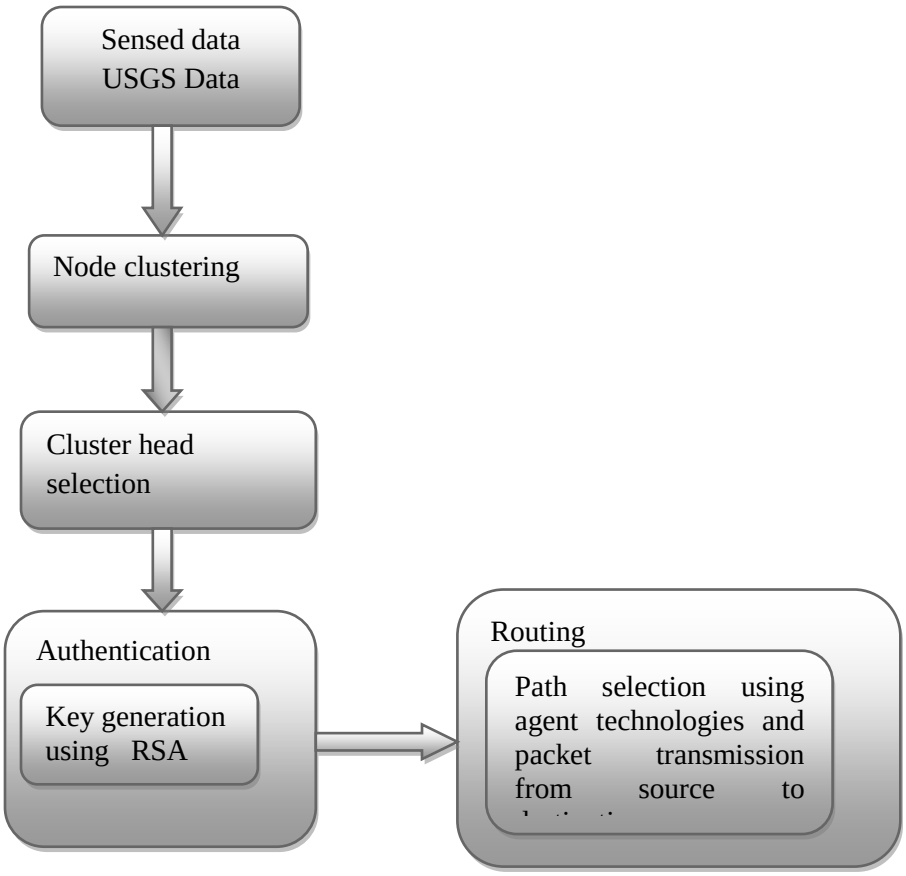

Figure: 1.Overall architecture of the proposed system

4.1. Network Model for agriculture

A sensor nodes as well as a sink node has been present in the network environment and the sensor nodes are randomly dispersed in the field. The data has been identified and the knowledge base is updated by the sensor nodes. Sensory devices like pH, moisture, temperature the salinity of soil, camera, an agent platform with stable as well as ambulant agents and other have been present in the Sensor node. It is said that on the basis of the communication range a sensor node forms a cluster. And various sensory devices have been connected in the sensor node. The identified message is transmitted to sink node through cluster head with the help of the multi-hop technique, once the information is identified by the sensor node.
Figure 1.illustrates the network environment.

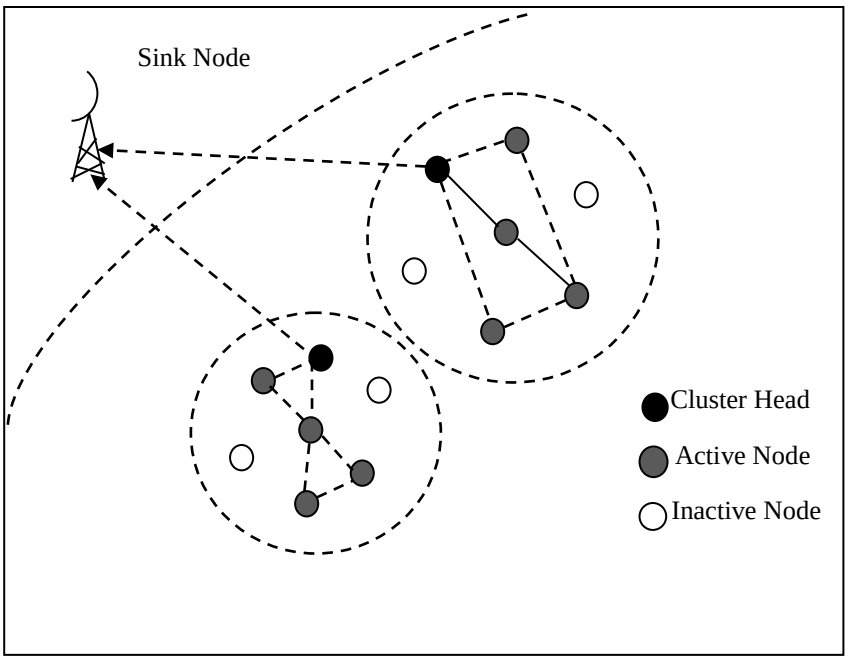

Fig.1.Network Environment

4.2. Soil

As a mix of various aspects like the salinity of soil (soil electric conductivity), moisture in the soil, temperature of the soil, PH in the soil and many more as stated, the soil can be measured. And on the basis of geographic region of agricultural land and the type of crop cultivated in that land, the values of soil aspects like soil PH and soil electric conductivity can differ [18].

4.3. Cluster head selection using Hybrid cuckoo search and genetic algorithm

The optimal cluster heads for Communication range based node clusters has been determined by this hybrid optimisation. The obtained message is transmitted to sink node through cluster head with the help of multi-hop technique, at once the information is acquired by the sensor node.

Cuckoo search algorithm

There are many types of nature-inspired population on the basis of stochastic global search meta-heuristic algorithm, which has been developed; Cuckoo search (CS) algorithm is one among them. As the name suggests this algorithm has been designed on the basis of as well as a combination of certain aspects of real time bird species such as, the merge of the obligate brood-parasitic trait of some cuckoo species with the Lévy flight trait of some birds and fruit flies. One peculiar trait about these species is that, they have wondrous abilities such as, they lay their eggs in the nests of other birds (mostly different species), but the highlighted trait is that they efficiently choose the recently built nests and remove the eggs of the host bird, which in turn results in high hatching probability of their own eggs more than the host's egg. Even though, some of the host birds possess the ability to overcome this exploitative trait of cuckoos and push out the identified eggs of cuckoo or they build a fresh nest in a fresh location. To develop a new optimization algorithm, this resemblance of the cuckoo breeding is used [19, 20].It is not possible to build a computer algorithm based the system of nature with perfection. It is because they are complex in nature. In order to attain successful application of a computer algorithm, it is inevitable to simplify the system of nature to be inspired on. By three idealised conditions we can simplify the cuckoo breeding process:

1. At a time a cuckoo lays one egg, and puts it in a randomly selected nest of the host bird.

2. The eggs dumped in the nests with high quality of eggs will be carried over to the next generation.
3. The number of available host nests is constant, and a host will be able to identify a foreign egg (i.e., the cuckoo's egg here) with a probability $p_a \in [0, 1]$. On considering this, it is certain that the host bird will either throw the egg away or leave the nest to build a fresh nest in a different location.

The following cuckoo search strategy can be derived from the aforementioned rules:
1. Assume that the egg stored in a nest indicates the solution and at a time an artificial cuckoo is able to lay only a single egg.
2. In order to increase the rate of survival of their eggs (solution), the cuckoo bird searches the most desirable nest to dump the eggs (solution). Elitist selection process is applied, To make sure that only the high quality eggs (best solutions near to optimal value) which are more identical to the host bird's eggs have more possibility to develop (next generation) and become a mature cuckoo.
3. The number of host nests (population) is constant. The host bird identify the alien egg (worse solutions away from optimal value) with a probability $p_a \in [0,1]$ and these eggs are pushed away or the host bird leaves and built a new nest, in a different location. If not so, the egg will survive and will be alive for the next generation. New eggs (solutions) lay by a cuckoo determines the nest with the help of Lévy flights around the current best solutions.

Genetic algorithm

Genetic algorithm (GA) is a search technique uses random choice to lead a highly parasitic search, striking a balance between exploration of the feasible domain and exploitation of ''good'' solution. A simple GA basically has three operators: reproduction, crossover, and mutation. The action of survival-of-the-fittest selection is called as reproduction. Crossover is the fragmentary reciprocation between two parent strings to create two offspring strings [21, 22]. Mutation is the rare random conversion of bit values that creates non-recursive offspring. The simultaneous assessment of many solutions is the important trait of the GA.

The process for the application of this algorithm is given briefly by the following steps:
Step 1: Create a random initial population.
Step 2: Assess the fitness function for each individual in the current population.
Step 3: Check the default stopping criteria.
Step 4: Create a new generation by performing Reproduction, crossover, and mutation on the current population.
Step 5: Repeat Steps 2 to 4 till stopping criteria. For simulating the processes in a natural system mandatory for evolution the basic concept of GA is designed, especially those that adopt the principles initially introduced by Charles Darwin of survival of the fittest. Many learn, assess, and implement GA in various fields in the universe engineering [23].

Hybrid cuckoo search and genetic algorithm

To amalgamation of the pros of both cuckoo search as well as genetic algorithm has been the initial ignition to design a hybrid CS-GA method. Regarding the selection and the proper utilization of optimization method, many times it has been a confronting process for identifying a better solution for an optimization issue.

Initially, the arbitrary distribution of the entire host nests belongs to the initial population have processed across the search space. A solution has denoted by an egg, which has stocked in a nest. Similarly, each nest solely includes one egg/solution in initial stage. The composition of RRAP solution includes integer parts that denote the redundancy level, whereas real parts demonstrate the reliability of components. Thus, it has defined as $(Y, s) = \{(y_1,y_2,y_3,y_4, \ldots ,y_n), (s_1, s_2, s_3, s_4, \ldots , s_n)\}$. The representation of a solution. An integer v_i within [0, -1] has been denoted by the l binary digits for number

of redundancy x_i, which generates the number of redundancy with in [1,u_i] as $Y_i = \langle 1 + v_i(u_i - 1)/(2^l - 1) \rangle$. In order to rounding the value to the near integer, the $\langle . \rangle$ operator has applied. Like l 'binary digits, the k binary digits for component reliability.

To generate a new population, the Genetic operators (selection, crossover, and mutation) has exploited. The Roulette Wheel selection has utilized to select two parents among the population, in which the recombination/crossbreeding has employed to generate two new offspring (eggs). In the process of recombining the genetic material in two parent cuckoo, Crossover has involved to conduct the parents' characteristics to the two eggs generated by them.

Here, the involvement of single point crossover approach enables each cuckoo to mutate by itself with the intention of sustaining the variance between the population and inhibit premature convergence. At this point, the flip mutation strategy has applied, in which a random walk has induced across the search space solely by mutation. Post-process of every crossover and mutation, such type of elitism has been processed, by which the population has chosen and sustained with optimal solutions. The new cuckoo egg replaces the parents from their place and occupies it, if it is more potential than the parent; else the place will be retained by the parent cuckoo bird in the crossover approach.

During the process of mutation, the newly mutated cuckoo egg occupies the place of old cuckoo bird, if it is more efficient than the latter. On the contrary, the egg being poor conditioned, it has considered to be found as an alien egg and has detached from the nest. Thus, the assurance has given by the elitist method to always keep the optimal candidate solution in the next generation.

$$X_{i,n+1} = \begin{cases} y_i iff(y_i) > f(x_i, n) \\ x_{i,notherwise} \end{cases} i = 1,2, \ldots . N \qquad (1)$$

Preceding with the generation of new population, the eggs that have survived to become a mature cuckoo bird, after which these mature birds immigrate to a better atmosphere for their lifetime through Lévy flight, and other manners in real life. Adding to that, the birds have restricted to construct the nests in the destination area due to the limited capacity over there. Throughout this study, the best cuckoo chosen from the current population will do the Lévy Flight to produce new egg (solution) in a stochastic manner.

$$x_i(t+1) = x_i(t) + \propto \oplus Levy(\beta) \qquad (2)$$

Here, the step size has denoted by a > 0 that must be associated to the measurement of PoI. In order to take the difference between solution qualities,

To reduce the intra-cluster compactness accompanying minimal distance connecting the nodes in the same cluster is the aim of fitness function, adopted by hybrid optimization.

Initiate

Objective function f(**Y**);

Step 1: Initialization. Define the generation counter t=1; initialize nodes (population) randomly.

Initialize Np number of nodes randomly each have minimum distance between inter clusters (Initialize Np number of host nests randomly each host nest have an egg corresponds to a potential solution to the given problem);

Step 2: Fitness evaluation. Assess distance amid nodes in the same cluster (fitness f(Y));

While (t< Max Generation) or (stop criterion); /**New population** /

Create new population through genetic operators (selection, crossover and mutation)

Assess fitness the best individual perform Lévy flight(The best node with minimum distance)

Create a new solution (say x_{new}) via Lévy flights;

Assess its quality/fitness Fx_{new};

Select a solution (say Y_j) randomly among Np_{new} and evaluate its fitness (Fj);

if(Fx_{new} < Fj) then

Switch j by a new solution;

end if

Archive the best solution;

t = t+1;

Step 3: end while

Step 4: Recover the best solution among the current best solution stored in each generation

End

The optimal cluster heads have chosen according to aforementioned strategy, subsequently it has been involved to transmit the data from sensors to sink/base station.

4.4. Key Generation and Authentication Using RSA Algorithm

The Key Generation and distribution have processed by exploiting RSA cryptography technique in this study, concerning the privacy, and authenticity, as well as prohibition of all sort of attacks. RSA algorithm has known to be a asynchronous cryptographic algorithm, in which a couple of keys have involved, namely public and private keys. Among them, a private key takes place to process the data encryption, whereas the decryption of data has carried out by public key. Generating the couple of keys is the primary step during the function [24]. Post-generation of keys, the public key requires to be distributed across transitional nodes and towards the destination.
STEP1: Select 2 large prime numbers p and q at random
STEP2: Acquire n = p * q
STEP3: Euler quotient function of n, z = (p – 1) (q – 1)
STEP4: The public key, e should be chosen in a specific way, where it has to be less than n; therefore, e & z are relatively prime
STEP5: Select the private key, d; hence, if d is divided by z remainder obtained is equal to 1 (d = e inverse mod z).

ENCRYPTION

The data encryption has performed through Encryption module in order to transfer it to the sink. The public key acquired from the process of key generation, and from the distribution module has utilized and encrypted by the sender. To select the path, the subsequent Ciphertext has been transferred to the destination through employing the agent technologies.

Method

Step 1: Give the data (M) and private key (e) as input
Step 2: Convert M into a number m. Hence, m smaller than n by an agreed-upon reversible protocol, which is termed as a padding scheme.
Step 3: Estimate the ciphertext c as

$$m=c_d \bmod n. \quad (3)$$

DECRYPTION

Method

Step 1: Give the ciphertext c and public key d as input
Step 2: Determine cd
Step 3: Estimate cd mod n
Step 4: Assess result is indigenous text m [25].

4.5. Agent technology

Once the data has recognized, RSA-driven keys will encrypt it. Throughout this research, Agent technology has employed to choose the optimal path across clusters member to cluster heads, and in the way through cluster head to sink node as regards the transference of encrypted data. The node that necessitates the data from various sensor nodes is called sensor nodes that provides the ways to acquire the data from every node/a set of nodes available from sink node that has been provided by the neighbour cluster head node. An agent platform and the proposed agent information transformation model have existed in each node of WMSN. In this study two types of agencies have suggested, namely Sensor node agencies, and sink node agencies.

4.5.1. Sensor node agencies

The sensor manager agent, sensor knowledge base, and path finding agent are the components of Sensor node agencies.

Sensor manager agent (SMA)

All the sensor nodes of WMSN possesses SMA which has known to be a stable agent. It is accountable to synchronize the functions of the agents among themselves as well as outside agents, besides it generates the node knowledge base (NKB) and path finding agent (PFA). The observed data, capture time and signal strength have been updated to the NKB by SMA. It contrasted the recognised value from threshold values existed in NKB and elucidates the circumstances. The arbitrary midpoint connecting the source and destination node; and intermediate nodes across the reference axis amid the source and the destination node has been estimated, if the context has identified. And it evaluates hop distance factor too. No data will be transferred to the sink while the SMA is in sleep mode. If the battery is running out, the status of the battery will be sent to the sink node, by keeping the track of battery consumption. The node details, like node id, location detail, environment, and signal strength information will be transferred to the sink node, at the instance of higher signal strength which is superior to the default threshold value defined by the sink.

Node knowledge base (NKB)

The SMA reads and updates this knowledge base. The node id, input values, sensing time, active mode/sleep mode, threshold values, bandwidth required to transfer the signal strength, and location of the node has been accommodated by NKB.

Path finding agent (PFA)

Each sensor node includes PFA that has known to be a mobile agent. The SMA produces PFA and its clone for route discovery, once the context has identified. The detail of each node, namely node id, bandwidth, residual energy, hop distance, and hop count has been accommodated by it, which has transferred to the cluster head.

4.5.2. Sink node agency

Agents such as manager agent, sensor knowledge base, and query agent have included in the sink node agency.

Manager agent (MA)

The sink node of WMSN contains this agent, which is a static one. It is being liable to synchronize the operations of the agents among themselves as well as the outside agents, besides generates sink knowledge base (SKB), query agent (QA). If required, it observes and updates the SKB. From the SKB, the MA looks for the locations detail of active sensor node and creates the better routes. By keeping the track of network either by alert alarm or by updating it in the user database, the data has transmitted to the user, once the context has been identified.

Sink knowledge base (SKB)

MA is able to read and update this knowledge base. The details of the node id, context information, sensing time, signal strength, the bandwidth needed for transferring the image of each active node, available network bandwidth, and locations of the active nodes has been archived here. In the process of QA, the entire details from sensor nodes must be transmitted, whenever the query has triggered from sink node. Subsequently, the sensor nodes have split into clusters. Every sensor node of the cluster transmits the recognized information towards respective cluster head. Then consolidation of the data from all the cluster heads has been done, in order to transmit it to sink node. This consolidation happens at the farthest cluster and the farthest cluster has been determined on the basis of the Euclidian distance.

Agent Interactions,

In the course of context recognition, the information gathering is accomplished through geographical distribution of sensor nodes all over the field. The cluster head is chosen through the utilization of LEACH protocol and passes this information to the entire sensor nodes. The signal strength is a key factor in deciding the sensor nodes to which it is appropriate. The pictorial representation of Agent Interaction sequences of the projected scheme is shown in Fig. 2.

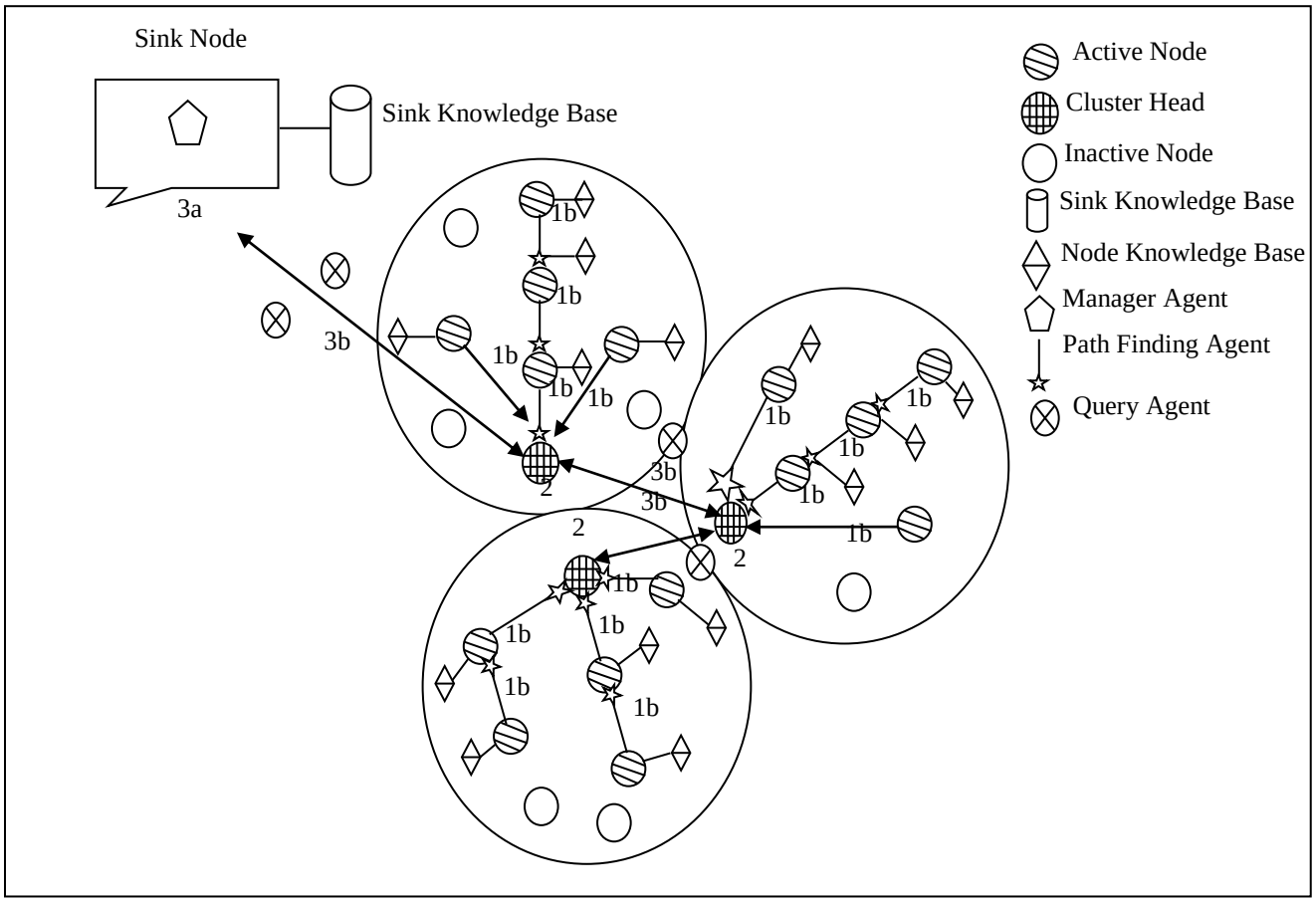

Fig. 2 .Agent Interactions

1. The interaction information of Senor Node agent is outlined below

a. The updating of the information sensed by the Sensor node is done any time the context is identified,

b. The active status is sent by the SMA to its cluster heads.

2. The PFA and its clone for route discovery is generated by SMA as well the sensed information is sent to the cluster head. The storing of all the sensor nodes information in the cluster Head is done.

3. The elucidation of Sink node agent interaction information is as follows:

a. The QA is generated by the MA which in turn gives the routing information.

b. The gathering of information is done after QA attaining the farthest cluster head and Euclidean distance plays a key role in making decision for the farthermost cluster. The information is gathered from cluster head once the QA touches subsequent nearest cluster. In a similar manner, the information from all sensor nodes is gathered by

nQA and fused thereby attaining the sink node.

4. Then updating of SKB is done by MA of sink node and offers the information of all the sensor nodes to the consumer. MA performs essential action through turning on/off the sprinkler or motor whenever neccestiated. \\

The information is stored after decryption of data once the data is received by the sink.

5. RESULT AND DISCUSSION

The proposed approach is implemented and validated by utilizing NS2 tool and the validation id done by comparing the projected approach i.e Improved Security with RSA method (ISRSA) with that of the prevailing approach such as Decision support system (DSS), Multi agent based context aware information gathering (MACAG) methods, Multi Improved Ant Colony Optimization and information gathering (IACOIG) and IECC protocol pertaining to packet delivery ratio, End To End Delay, Energy,

Average energy consumption for the dataset of USGS. The data and metadata accompanying with the journal article is encompassed in the U.S. Geological Survey Data Release.

The nest survival is a key factor for the Parental incubation behaviour which is regarded as a critical demographic process in avian population dynamics, and the various life history breeding stratagems impacts on behavior variations across species. The mixing colonies, behavioral mechanisms are the various advantages of nest survival which are likely lacking. The investigation is carried out for parental incubation behavior utilizing video-monitoring techniques on Alcatraz Island, California, of black-crowned night-heron Nycticorax nycticorax (hereinafter, night-heron) in a mixed-species colony with California gulls Larus californicus.

Table: 1. Performance Comparison Results with different methods

METHODS	Packet Delivery Ratio (Milli sec)		
	10	20	30
DSS	0.0185	0.0058	0.0028
MACAG	0.0187	0.0056	0.0006
IACOIG	0.0191	0.0077	0.0002
DES	**0.0199**	**0.0087**	**0.0002**
ISRSA	**0.0205**	**0.0097**	**0.0002**

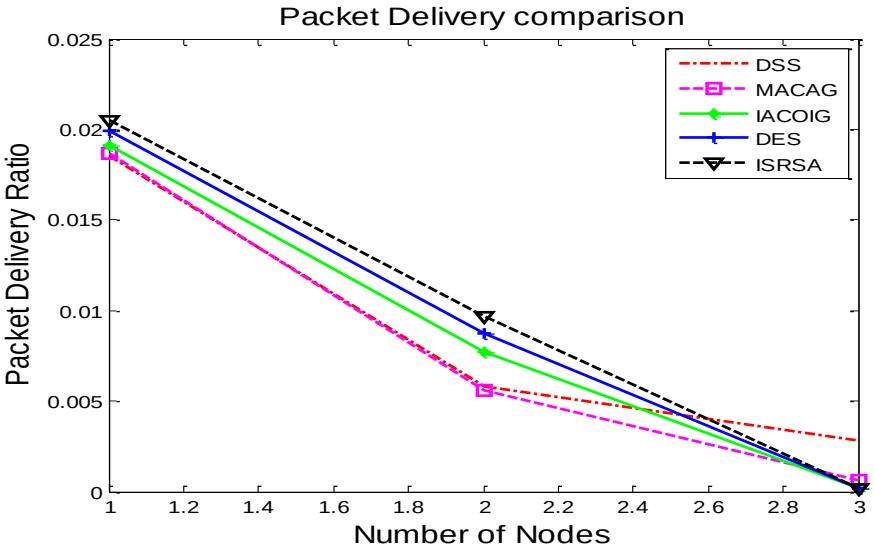

Figure: 3. Packet delivery ratio

Figure 3 narrates about the packet delivery ratio of the suggested ISRSA approach in contradiction to the prevailing DSS, MACAG, IACOIG and IECC approach, while taking No of nodes and Packet delivery ratio in X-axis and Y-axis respectively. The Keys in RSA algorithm are produced by utilizing prime numbers where factorizing through this parameter is a difficult task and offers improved security. The suggested ISRSA model delivers **0.0205** Packet delivery ratio which is highest comparatively with that of the prevailing DSS, MACAG, IACOIG and DES approaches whose Packet delivery ratio are only 0.0185, 0.0187, 0.0191, 0.0199 and 0.0205 respectively.

Table: 2.Assessment of end to end delay with the prevailing approaches

METHODS	End To End Delay (MilliSec)		
	10	20	30
DSS	2.6037	2.6080	2.7623
MACAG	1.4611	1.3955	1.6032
IACOIG	1.3591	1.3595	1.5132
DES	1.2891	1.3245	1.3992
ISRSA	1.2041	1.2897	1.2789

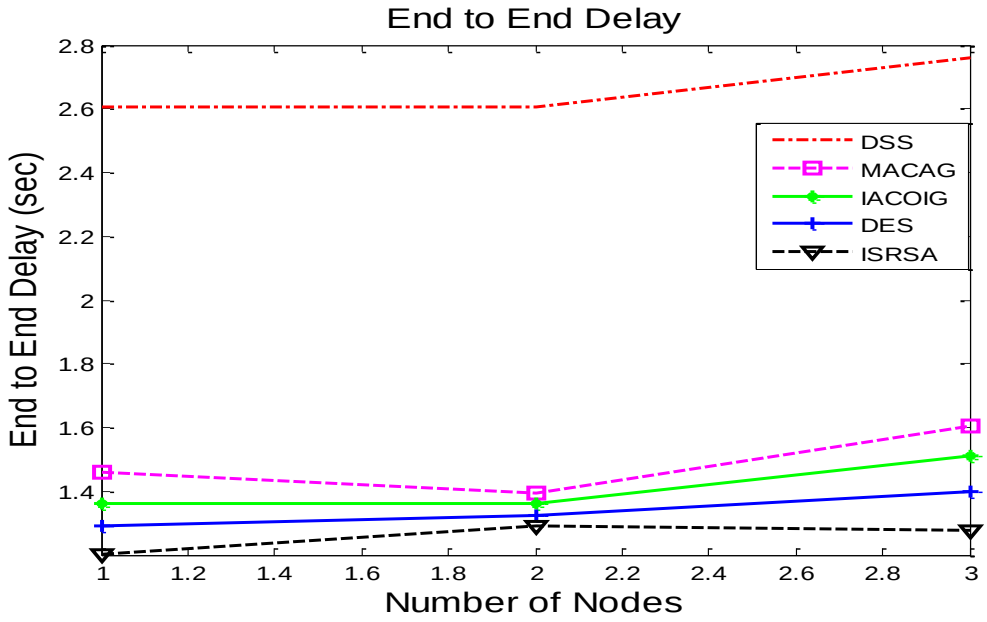

Figure:4. End to end delay in Milliseconds.

Figure 3 describes about the End to end delay of the suggested ISRSA approach in contradiction to the prevailing DSS, MACAG, IACOIG and IECC approach, while taking No of nodes and End to End delay values in X-axis and Y-axis respectively. The suggested ISRSA model provides lowest End to end delay results of 1.278(ms) in contradiction with that of the prevailing DSS, MACAG, IACOIG and DES approaches whose End to end delay are 2.762 (ms), 1.603 (ms), 1.5132(ms) and 1.3992(ms) respectively. The agent technology along with manager agent is greatly deployed in obtaining the shortest path from the cluster to the head and from the sink to the head ,thereby obtaining lowest delay.

Table: 3.Comparison of the Total Energy Consumption with the other methods

METHODS	Total Energy Consumption		
	10	20	30
DSS	0.1275	0.0229	0.0903
MACAG	0.0577	0.0917	0.0072
IACOIG	0.0323	0.0247	0.0111
DES	0.0243	0.0202	0.0089
ISRSA	0.0201	0.0199	0.0080

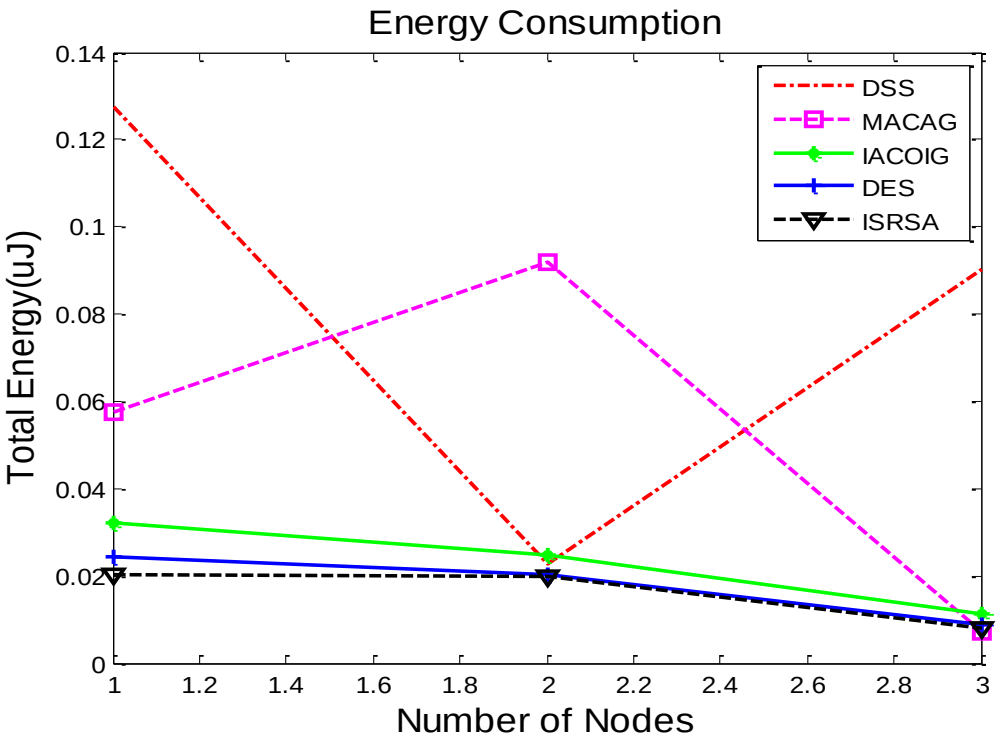

Figure: 5.Total Energy consumption results in mill Jules

The energy consumption of the suggested ISRSA method pertaining to the existing DSS, MACAG, IACOIG and IECC technique is shown in figure 5 while considering No of nodes and Total Energy consumption values in X-Axis and Y-axis respectively. This research greatly exploits hybrid cuckoo search for selection of cluster heads for the nodes in the network and optimized heads is obtained through the fitness function parameter of the cuckoo search which is utilized to attain reduced energy consumption by miminum distance amid the inter clusters. The suggested ISRSA model provides lowest Energy consumption results of 0.0201(mj) in contradiction with that of the prevailing DSS, MACAG, IACOIG and DES approaches whose Energy consumption are 0.1275 (mj), 0.0577 (mj), 0.0323 (mj) and 0.0243(mj) respectively.

Table: 4.Performance comparison results with different methods

Message size (mb)	Encryption time				
	DSS	MACAG	IACOIG	DES	**ISRSA**
20	5600	4800	4100	3800	3290
40	5500	4555	3960	3400	3100
60	4880	4200	3700	3150	3045
80	4690	4150	3400	3050	3005
100	**4500**	**4050**	**3250**	2930	2980

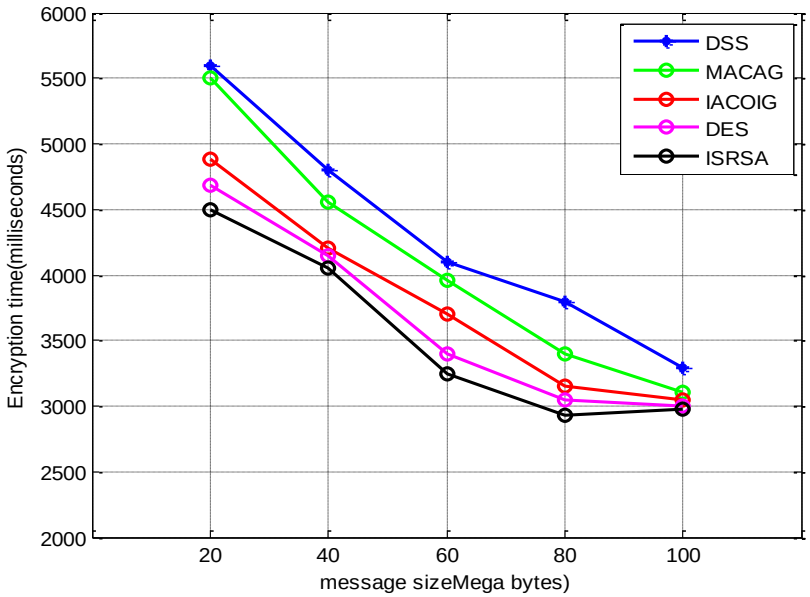

Figure:6. Encryption time vs message size in mega bytes

Figure 6 describes about the Encryption time vs message size in mega bytes of the suggested ISRSA approach in contradiction to the prevailing DSS, MACAG, IACOIG and IECC approach, while taking message size and Encryption time values in X-axis and Y-axis respectively.

Efficiency of the proposed ISRSA method is shown via comparing this with the existing DSS, MACAG, IACOIG and IECC method in terms of Attack Detection Accuracy. In the above figures No of malicious nodes are taken as X-Axis and attack detection accuracy values are taken as Y.From the results it concludes that the proposed ISRSA model produces 2980(ms)higher detection accuracy results whereas existing DSS, MACAG, IACOIG and DES methods produces only 3290 (ms), 3100 (ms),3450(ms) and 3005 (ms) respectively.

6. CONCLUSION AND FUTURE WORK

The Peculiar Characteristics of Wireless Sensor Network is its security due to the sensitivity of data gathered and susceptibility of the network. Various researches are being carried out to secure against different threats in WSN by suggesting enormous methodologies. The cuckoo search with genetic algorithm is greatly utilized for cluster head selection expending minimal energy consumption. RSA algorithm is involved in encryption of sensed data for substantiation to avoid attack through creation of public and private keys for all nodes in the network. Path Finding Agent (PFA) and key authentication has its influence on transmitting the encrypted information to the cluster heads by means of sensor nodes. Query Agent (QA) supports in aggregating the information received by the sensor nodes in the field through cluster head before transporting to the sink node and as a final point decryption of data is achieved through same key. The Proposed approach is validated through experimental results pertaining to improved security, packet delivery ratio and minimized energy consumption. The future work may concentrate in the field of agriculture by efficaciously constructing the prototypes with multiple challenges imposed.

REFERENCES:

1. Elhoseny, M. and Hassanien, A.E., 2019. Secure data transmission in WSN: an overview. In *Dynamic Wireless Sensor Networks* (pp. 115-143). Springer, Cham.
2. Wang, J., Cao, J., Ji, S. and Park, J.H., 2017. Energy-efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks. *The Journal of Supercomputing*, *73*(7), pp.3277-3290.
3. Kumar, S.A. and Ilango, P., 2018. The impact of wireless sensor network in the field of precision agriculture: a review. *Wireless Personal Communications*, *98*(1), pp.685-698.
4. 4.Ramdoo, V.D., Khedo, K.K. and Bhoyroo, V., 2019. A Flexible and Reliable Wireless Sensor Network Architecture for Precision Agriculture in a Tomato Greenhouse. In *Information Systems Design and Intelligent Applications* (pp. 119-129). Springer, Singapore.
5. Chlingaryan, A., Sukkarieh, S. and Whelan, B., 2018. Machine learning approaches for crop yield prediction and nitrogen status estimation in precision agriculture: A review. *Computers and electronics in agriculture*, *151*, pp.61-69.
6. Kochhar, A. and Kumar, N., 2019. Wireless sensor networks for greenhouses: An end-to-end review. *Computers and Electronics in Agriculture*, *163*, p.104877.
7. AdelineSneha, J., Chakravarthi, R. and Glenn, J.A., 2016, March. A review on energy efficient image feature transmission in WSN for micro region pest control. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 4859-4862). IEEE.
8. Rajasekaran, T. and Anandamurugan, S., 2019. Challenges and Applications of Wireless Sensor Networks in Smart Farming—A Survey. In *Advances in Big Data and Cloud Computing* (pp. 353-361). Springer, Singapore.

9. Jha, K., Doshi, A., Patel, P. and Shah, M., 2019. A comprehensive review on automation in agriculture using artificial intelligence. *Artificial Intelligence in Agriculture*.
10. .Affrin, K., Reshma, P. and Kumar, G.N., 2017, April. Monitoring effect of air pollution on agriculture using WSNs. In *2017 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR)* (pp. 46-50). IEEE.
11. Ali, R., Pal, A.K., Kumari, S., Karuppiah, M. and Conti, M., 2018. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future Generation Computer Systems, 84, pp.200-215.
12. Sahitya, G., Balaji, N. and Naidu, C.D., 2016, July. Wireless sensor network for smart agriculture. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 488-493). IEEE.
13. Liu, N., Cao, W., Zhu, Y., Zhang, J., Pang, F. and Ni, J., 2016. Node Deployment with k-Connectivity in Sensor Networks for Crop Information Full Coverage Monitoring. Sensors, 16(12), p.2096.
14. Parganiha, P. and Kumar, K.A., 2018. An Energy-Efficient Clustering with Hybrid Coverage Mechanism (EEC-HC) in Wireless Sensor Network for Precision Agriculture. Journal of Engineering Science & Technology Review, 11(3).
15. Mehetre, D.C., Roslin, S.E. and Wagh, S.J., 2019. Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Computing, 22(1), pp.1313-1328.
16. Wu, J., Ota, K., Dong, M. and Li, C., 2016. A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. *IEEE Access*, *4*, pp.416-424.
17. Sujihelen, L. and Jayakumar, C., 2018. Inclusive elliptical curve cryptography (IECC) for wireless sensor network efficient operations. *Wireless Personal Communications*, *99*(2), pp.893-914.
18. Agrawal, N., Kumar, A., Bajaj, V. and Singh, G.K., 2017. High order stable infinite impulse response filter design using cuckoo search algorithm. International Journal of Automation and Computing, 14(5), pp.589-602.
19. Shehab, M., Khader, A.T. and Al-Betar, M.A., 2017. A survey on applications and variants of the cuckoo search algorithm. Applied Soft Computing, 61, pp.1041-1059.
20. Khare, M.D. and Yadav, C.S., 2017, August. Secure data transmission in cloud environment using visual cryptography and genetic algorithm: A review. In 2017 International Conference on Innovations in Control, Communication and Information Systems (ICICCI) (pp. 1-4). IEEE.
21. Abdelaziz, M., 2017. Distribution network reconfiguration using a genetic algorithm with varying population size. *Electric Power Systems Research*, *142*, pp.9-11.
22. Xu, R. and Cai, K., 2019. Solving Airport Gate Assignment Problem Using an Improved Genetic Algorithm with Dynamic Topology. In *Recent Developments in Intelligent Computing, Communication and Devices* (pp. 877-884). Springer, Singapore.
23. Singh, A., Awasthi, A.K. and Singh, K., 2016. A key agreement algorithm based on ECDSA for wireless sensor network. In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics (pp. 143-149). Springer, New Delhi.
24. Abirami, R., Manimegali, R., Vidhyadharshini, M., SenthilKumar, A.M., Vijaykumar, M.S. and Santhiya, S., 2018. Data Integrity Protection for Wireless Sensor Network Using Key Establishment Scheme. Journal Impact Factor, 2, p.2.
25. Fu, J., Hua, J., Xu, Z., Lu, W. and Li, J., 2018, July. Improved RSA Localization Based on the Lagrange Multiplier Optimization. In International Conference on Machine Learning and Intelligent Communications (pp. 632-640). Springer, Cham.