ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 10, October 2019

Energy Optimized Secured Routing Protocol for Attack Mitigation in Wireless Sensor Network

K.G. Maheswari, C. Siva

Assistant Professor (Senior), Department of IT, Institute of Road and Transport Technology, Anna University, Erode, Tamil Nadu, India

Professor, Department of Information Technology, Nandha Engineering College, Erode, India

ABSTRACT: Energy optimized and secured routing consumes a significant part in the remote sensor organization. There are different examination strategies has been presented before for the data transmission in the network. In our past examination work it is accomplished by presenting the strategy Detection and Mitigation System (DMS) which plans to distinguish the routing attacks occurring on the network. Anyway this exploration focuses on trust esteem alone to separate the noxious aggressor nodes from the certifiable nodes. This is engaged and settled in the proposed research work by presenting the strategy Secured Energy Efficient Attack Mitigation System (SEEAMS). In this research work, initial route path establishment is done using dijkstrakth shortest path algorithm. Once the population is initialized fitness value will be evaluated for each population of route paths. Based on calculated fitness value of each route path, route choice probability will be calculated. The route path with maximum probability will be elected for the optimal data transmission. To ensure the optimal route path selection, this work adapted the Hybrid Artificial Bee Genetic Colony based route path selection. To secure the data transmission from the malicious attacks, in this work Intrusion Detection System is integrated in the sensor nodes which will monitor and predict the malicious patterns occurring on the data's that are transmitted. The general assessment of the examination work is finished in the NS2 tool from which it is demonstrated that the proposed research work accomplishes preferable execution over the previous exploration strategies.

KEYWORDS: Route path population, fitness value, route choice probability, artificial bee colony, genetic algorithm, intrusion detection, cooperative engine

I. INTRODUCTION

Wireless sensor network is a communication of sensor nodes with a distant design [1]. The hubs will notice the climate and forward it through multi bounce way in the affiliations [2]. With quick decrease in cost of sensors, WSN is utilized in various applications like creating, current security, typical life seeing, and so on [3]. Normal WSN incorporates hubs related with far off framework [4]. Most sensor networks are unattended with sensor hubs being loaded up with batteries [5].

Because of perceiving, tuning in, managing, transmission and get-together of packs, the battery energy is consumed and these cycles are not made game plans for ideal way, the energy channels at speedier rate and hubs turns out to be dead [6]. The hub disappointment doesn't just decrease the perceiving considerated locale, yet besides influences the steering [7]. The organization openings made in the affiliation disturbs the multihop directing and confines the affiliation undaunted quality. Considering unattended nature, it isn't possible for battery trade for depleted hubs [8]. In the ongoing circumstance reasonable utilization of energy is the best procedure for expanding the lifetime of hubs [9]. Because of Wireless construction, WSNs are inclined to different assaults like message drops, message changing, Denial of organization through message flooding, and so forth [10]. Affirmation of these assaults and moderation from these assaults is significant for steadiness of usages utilizing the sensor affiliation. Executing a higher unusualness security procedure consolidates higher energy utilization for managing at sensor center points and this hence decreases the lifetime of the center points [11].

Recent explores in WSN have proposed various routing protocols, among them energy is most viewed as objective in their routing technique [12]. Routing protocol has the majority of the consideration since it can shift from the organization design and its application. In micro sensor networks it can contain hundreds or thousands of detecting nodes. It is fundamental to create modest and energy productive sensor nodes. Conversely, with IP-based communication, which relies upon worldwide addresses as well as routing measurements of hop counts, the sensor nodes normally need global addresses [13]. The essential test in planning WSN is the arrangement of the functional, and the non-useful, for instance, information latency and integrity separately.

Energy proficiency and security of information stayed all the time as open examination issues in WSN [14]. A large portion of the battery power is consumed by routing progress and in this way the existence of an organization predominantly relies upon the proficiency of its routing protocol. The more the energy-proficient routing of an organization, the more drawn out will be its network lifetime. Besides, the transmission of information to objective without being caught or manufactured by the attackers is likewise a fundamental issue. There are verities of protocols intended for energy-effective routing and securing them.

The primary objective of this examination work is to guarantee the ideal and reliable routing through which secured transmission can be laid out. Here data transmission is guaranteed by adjusting the intrusion detection framework which will screen and anticipate the pernicious patterns present in the communicated information. And furthermore reliable and energy proficient routing is ensured by picking the more ideal route paths from the climate utilizing advancement strategies.

II. RELATED WORKS

Santhosh Kumar et al [15] executed Secured-Selective Design Relay Inquiry Protocol (S-SELDRIP) which gives the ideal coordinating through various bob endorsement during information spread. The opportunity and ampleness of S-SELDRIP plot have been explored by considering expected deficiencies during the information spread and how much the proposed create can get past them.

Prithi et al [16] interweaved the Deterministic Finite Automata (DFA) and Particle Swarm Optimization (PSO) for obstruction ID and the information transmission is done securely by picking and following the strong course. A LD2FA (Learning Dynamic Deterministic Finite Automata) is familiar with refine the exceptional quality of the affiliation. Thus, LD2FA - PSO gives the data about the center, pack and course appraisal for disclosure and ejection of attackers so the information transmission is done in an energy able way through the most ideal way.

Thangaramya et al [17] introduced cushy rule and assembling based guiding technique with trust appearing and anomaly recognizing evidence for registering the center points looking with the correspondence. Besides, a feathery common rule and distance-based peculiarity divulgence assessment is moreover proposed in this work for seeing the pernicious center points from different center points inside each social occasion of the affiliation and has been utilized in the gotten coordinating show.

Selvakumar et al [18] introduced directing show called Energy Aware Secured Algorithm for Routing which is secure by utilizing a Trust based technique and is Energy effective simultaneously. Thus, another energy able show utilizing Fuzzy C-recommends has been proposed in this work. Moreover, a changed intersection tree approach is applied here to perceive the base distance way between the source and objective center and consequently an ideal and got way is picked.

Haseeb et al [20] introduced an IoT-based WSN structure as an application to savvy agribusiness including different course of action levels. As an issue of some significance, country sensors get pertinent information and close a lot of gatherings heads considering multi-measures choice capacity. Likewise, the strength of the signs on the transmission joins is evaluated while utilizing sign to clatter extent (SNR) to accomplish steady and effective information transmissions. Moreover, security is guaranteed for information transmission from country sensors towards base stations (BS) while utilizing the repeat of the direct congruential generator.

Haseeb et al [21] developed an energy-convincing and secure directing show (ESR) for obstruction abhorrence in IoT considering WSN to construct the affiliation period of time and information relentlessness. Right away, the proposed show makes different energy-able gatherings thinking about the innate characteristics of centers. Also, considering quite far based Shamir secret sharing course of action, the steadiness and security of the material data among the base station (BS) and it are accomplished to accumulate head. The proposed security technique presents a light-weight answer for changing with impedances made by noxious centers.

Sarkar et al [22] proposed firefly with cyclic randomization for picking the best assembling head. The affiliation execution is stretched out in this technique when stood apart from the other standard systems. The bundle head is picked so it is spatially enough nearer to the base station as well as the sensor centers. Consequently, the time deferral can be widely lessened. As needs be, the transmission speed of the heaps of data can be expanded.

Srivastava et al [23] proposed rate-careful blockage control technique to the extent that bundle directing to decrease energy utilization all through the affiliation. Rate control process decreases the deferral to cultivate association life time for immense spread period furthermore. All along, centers are accumulated by the cross variety K-means and Greedy best first pursuit system. Beginning there, the rate control is performed utilizing firefly improvement structure which is reasonable for high group transport extent. At last, bundles are sent with most preposterous throughput utilizing Ant Colony Optimization-based coordinating.

Sajwan et al [24] presented a method which impacts both level and moderate directing strategies for expanding energy efficiency. It allocates some ideal number of hubs as bunch head to frame groups in the association. Inside gatherings, hubs take on multi-skip steering intend to talk with clsuter head, which on social event of stacks of info from all gathering people, sends the collected information along the precomputed way to the sink.

Dhand et al [25] gave practical transmission to this sort of affiliation, gathering related with secure coordinating is locked in to move the heaps of data securely to the endpoint. Information assembling and clustering help to bundle the affiliation and control transmission above during information transmission. Hybridization of K-suggests gathering calculation with Ant Lion Optimizer for get-together of centers and ideal CH confirmation is used for better energy ability. Nalinipriya et al[24,25] discuss the various attack detection, mitigation and prevention method in cloud environment.

III. SECURED ENERGY EFFICIENT RELIABILITY RANKIGN ROUTING

In this research work, initial route path establishment is done using dijkstrakth shortest path algorithm. Once the population is initialized fitness value will be evaluated for each population of route paths. Based on calculated fitness value of each route path, route choice probability will be calculated. The route path with maximum probability will be elected for the optimal data transmission. To ensure the optimal route path selection, this work adapted the Hybrid Artificial Bee Genetic Colony based route path selection. To secure the data transmission from the malicious attacks, in this work Intrusion Detection System is integrated in the sensor nodes which will monitor and predict the malicious patterns occurring on the data's that are transmitted.

3.1. PROBLEM FORMULATION

This research work is implemented over the network which is constructed as weighted graph represented as Graph = {Vertices, Edges}. Consider route path between the source node to the destination node is represented as $\mathrm{Path}_{\mathrm{T}}(\mathrm{source}, \mathrm{destination}_{\mathrm{i}})$ where $\mathrm{source}\in\mathrm{vertices}$ and $\mathrm{destination}\ \in\mathrm{vertices}$. Here multicast tree is represented as Tree (source, MulticastTree). Here for each edge ∈ E, cost function is assigned with five non negative real numbers. Here Cost function is represented as cost (edge) : Edge → NR^{+} where NR^{+} is non negative real number. Likewise, total cost of implemented multicast tree Tree(soruce, MulticastTree) can be calculated using equation (1)

$$\mathrm{Cost}\big(\mathrm{Tree}(\mathrm{source}, \mathrm{MulticastTree})\big) = \sum_{\mathrm{edge}\in\mathrm{Tree}(\mathrm{source},\mathrm{MulticastTree})} \mathrm{Cost}(\mathrm{edge}) \qquad (1)$$

Delay, bandwidth, packet loss of every route path $\mathrm{Path}_{\mathrm{T}}(\mathrm{source}, \mathrm{destination}_{\mathrm{i}})$ can be calculated as like given below:

$$\text{Delay}\left(\text{Path}(\text{source},\text{destination})\right) = \sum_{\text{edge}\in\text{Path}_\text{T}(\text{source},\text{destination}_\text{i})} \text{Delay (edge)} \qquad (2)$$

$$\text{Bandwidth}\big(\text{Path}(\text{source},\text{destination})\big) = \text{minimum}_{\text{edge}\in\text{Path}_\text{T}(\text{source},\text{destination}_\text{i})}\{\text{Bandwidth}(\text{edge})\} \qquad (3)$$

$$\text{Packet\_loss}\big(\text{Path}(\text{source},\text{destintion})\big) = 1 - \prod_{\text{edge}\in\text{Path}_\text{T}(\text{source},\text{destination}_\text{i})} [1 - \text{Packet\_loss}(\text{edge}) \qquad (4)$$

$$\text{Delay}_{\text{jitter}(\text{Path}(\text{source},\text{destination}))} = \sum_{\text{edge}\in\text{Path}_\text{T}(\text{source},\text{destination}_\text{i})} \text{Delay}_{\text{jitter}(\text{edge})} \qquad (5)$$

The issues faced in QoS multicast routing is given below. Consider the network is represented as Graph, where source node is represented as source and there are multiple destination nodes are available for multicast routing which is represented as MulticastTree. In this work, four different constraints are considered such as $\text{Delay}_{\text{maximum}}$, $\text{DelayJitter}_{\text{maximum}}$, $\text{Bandwidth}_{\text{minimum}}$, and $\text{PacketLossRatio}_{\text{maximum}}$. By considering these constraints, network solution needs to be identified which reduced cost function value which is represented as $\text{Cost}\big(\text{Tree}(\text{source},\text{MulticastTree})\big)$. The conditions are given below:

$$\begin{gathered}\text{DelayPath}_\text{Time}(\text{source},\text{destination}_\text{i}) \le \text{Delay}_\text{maximum} \qquad (6)\\ \text{Bandwidth Path}_\text{Time}(\text{source},\text{destination}_\text{i}) \ge \text{Bandwidth}_\text{minimum}\\ \text{Delay}_{\text{ jitterPath}_\text{Time}(\text{souce, destination}_\text{i})} \le \text{DelayJitter}_\text{maximum}\\ \text{Packet\_lossPath}_\text{Time}(\text{source},\text{destination}_\text{i}) \le \text{PacketLossRatio}_\text{maximum}\end{gathered}$$

3.2. ABGCA BASED RELIABLE ROUTING

In this work crossover Artificial Bee province with Genetic calculation has been used to guarantee the dependable steering result. The general handling stream of the examination work is displayed in the accompanying figure 1

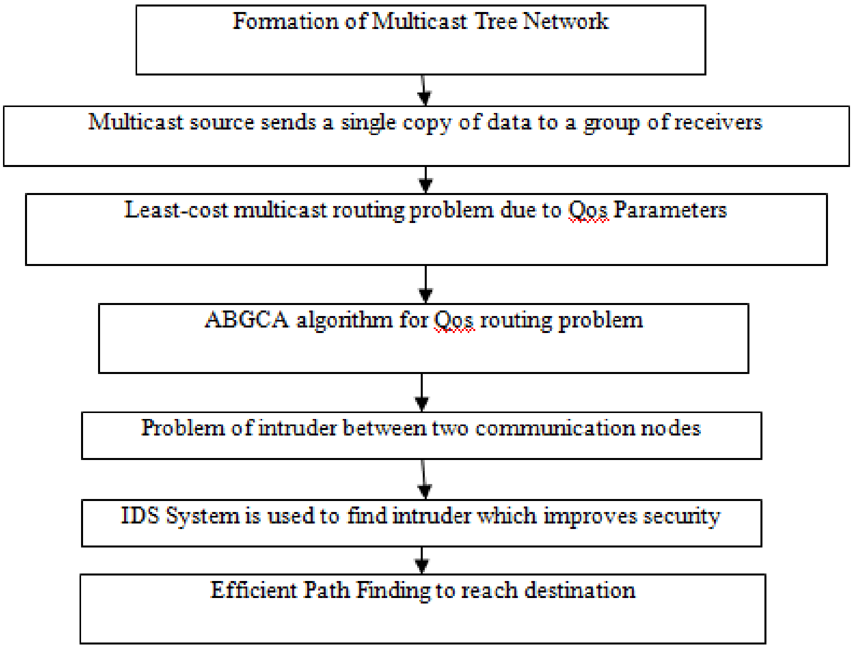

Formation of Multicast Tree Network
Multicast source sends a single copy of data to a group of receivers
Least-cost multicast routing problem due to Qos Parameters
ABGCA algorithm for Qos routing problem
Problem of intruder between two communication nodes
IDS System is used to find intruder which improves security
Efficient Path Finding to reach destination

Figure 1. Proposed Framework

3.2.1. INITIAL POPULATION

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 10, October 2019

For the better routing path establishment with lesser computation time, in this work Dijkstrakth shortest path algorithm has been introduced which will predict the shortest routing paths. Those shortest routing path will be considered as the initial population in the proposed hybrid optimization approach. Consider there are i number of destination nodes represented as $\mathrm{destination_i} \in \mathrm{MulticastTree}$. The hop count based cost will be estimated each route path between candidate nodes and destination nodes among them shortest path will be chosen using Dijkstra's algorithm. Those set of selected shortest route paths are denoted as $\mathrm{ShortestPath_i}$ as like given in Equation 7.

$$\mathrm{ShortestPath_i} = \{\mathrm{Path_i^1}, \mathrm{Path_i^j}, \dots \mathrm{Path_i^k}\} \qquad (7)$$

Where $\mathrm{Path_i^j}$ is denoted as an possible jth path between source node to the destination node. In our work, at the initial stage 20 possible route paths are considered which is mentioned as k=20. For example consider the multicast tree image shown in the following figure 2. Here one source node is considered which is node 1 and four destination nodes are considered which node 4, 6, 7 and 8. In table 1, $\mathrm{ShortestPath_i}$ to reach the destination node 7 is shown in the following table 1.

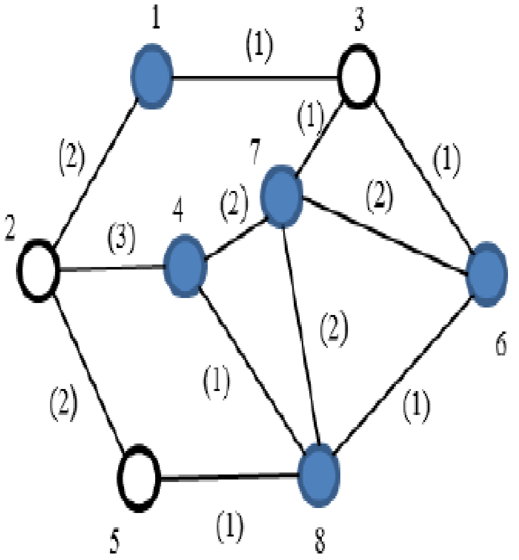


Figure 2. Topology of a Multicast Network

Table 1: $\mathrm{ShortestPath_i}$ for Node 7

Route number	Route list	Route cost
1	(1,3,7)	2
2	(1,3,6,7)	4
3	(1,3,6,8,7)	5
...	(1,...,7)	...
K	(1,...,7)	...

3.2.2. Fitness Function

The fitness values of each initialized population will be calculated for choosing most optimal route path. Here cost parameter is considered for the fitness evaluation where cost of each route path is calculated. Based on cost value estimated for each route path, cost matrix will be constricted. The fitness value is estimated by using the following equation 8.

$$fit_i = \frac{1}{1+f_i} \qquad (8)$$

The cost function is calculated f_i .

3.2.3. Calculation of fitness

Previous section described the process of calculating fitness value probability estimation. The main goal bee search algorithm is to find the most optimal route path which is established between the source and destination nodes. Here employee bee phase of the bee search algorithm will predict the optimal route path in terms of time and shortest path. Here the probability of choosing the optimal route path is calculated through its quality which is denoted as $\Delta f_{i,j}$. The quality calculation procedure is shown in the following equation 9.

$$\Delta f_{i,j} = \frac{\mathrm{Bandwidth(Route)}^{\lambda_{\mathrm{B}}\mathrm{andwidth}} + \mathrm{Energy(Route)}^{\lambda_{\mathrm{Energy}}} + \mathrm{Throughput(Route)}^{\lambda_{\mathrm{T}}\mathrm{hroughput}}}{\mathrm{Delay(Route)}^{\lambda_{\mathrm{D}}} + \mathrm{HopCount(Route)}^{\lambda_{\mathrm{HC}}} + \mathrm{DelayRatio(Route)}^{\lambda_{\mathrm{DelayRatio}}}} \qquad (9)$$

Here $\lambda_B, \lambda_E, \lambda_T, \lambda_D, \lambda_{HC}$ and λ_{DR} represent the weight factor values based on which optimal route path . Once the optimal route path is established reliable routing can be guaranteed.

3.3. PATH PREFERENCE PROBABILITY CALCULATION

Path preference probability plays an most important role in the route path selection process which involves monitoring all intermediate nodes. Path preference will be calculated whenever the request received to the source node for the data transmission. Probability estimation equation is shown in the following equation 10.

$$Path_{ijd} = \frac{[\tau_{ij}]^{\alpha 1}.[\mathrm{D}_{ijd}]^{\alpha 2}.[\eta_{ijd}]^{\alpha 3}.[\mathrm{Bandwidth}_{ijd}]^{\alpha 4}.[\mathrm{Energy}_{ijd}]^{\alpha 5}.[\mathrm{DelayRatio}_{ijd}]^{\alpha 6}.[\mathrm{Time}_{ijd}]^{\alpha 7}}{\sum_{\cdot k \in N_i} [\tau_{ik}]^{\alpha 1}.[\mathrm{Delay}_{ikd}]^{\alpha 2}.[\eta_{ikd}]^{\alpha 3}.[\mathrm{Bandwidth}_{ikd}]^{\alpha 4}.[\mathrm{Energy}_{ikd}]^{\alpha 5}.[\mathrm{DelayRatio}_{ikd}]^{\alpha 6}.[\mathrm{Time}_{ikd}]^{\alpha 7}} \qquad (10)$$

Where α1, α2, α3,α4, α5, α6 and α7 → adjustable parameter
Neighnour$_i$ → set of neighbour nodes
i and k → neighbour nodes through which destination can be reached.

The Qos Metric calculation procedure is given below:

$$\mathrm{Delay}_{ijd} = \frac{1}{\mathrm{delay(path\ (i,destination))}} \qquad (11)$$

$$\eta_{ijd} = \frac{1}{\mathrm{hopcount(path\ (i,destination))}} \qquad (12)$$

$$\mathrm{Bandwidth}_{ijd} = \mathrm{bandwidth\ (path(i,destintion))} \qquad (13)$$

$$\mathrm{Energy}_{ijd} = \mathrm{energy\ (path\ (i,destination))} \qquad (14)$$

$$\mathrm{DelayRatio}_{ijd} = \frac{1}{\mathrm{drain\ rate(path(i,destination))}} \qquad (15)$$

$$\mathrm{Time}_{ijd} = \mathrm{throughput\ (path\ (i,destination))} \qquad (16)$$

3.4. INTRUSION DETECTION SYSTEM FOR ATTACK PREVENTION IN NODE FOR SECURE PURPOSE

In this proposed work, IDS is upgraded to distinguish the sinkhole assault which holds the base station back from getting whole and accurate detecting information, thus makes a genuine danger to higher-layer applications. An ideal interruption distinguishing proof answer for the sensor network is inspected by recognizing the assaults by using coordinated IDS. Thusly, the examination work focuses principally on giving an answer for the past issues by administering the IDS, which brings about acquiring the ordinary condition of the organization. It gives the header data for whole hubs, which are joined in a solitary portable specially appointed organization and it will regulate the hub's activity. In the event that in the event that, any hub acts unusually or it gets to a greater number of assets than the typical one, it will be considered as a presumed hub for any assault succession perception. For the most part, procuring the updates through the speculated hubs and it will be registered. Multicasting arrangements will be picked to recognize the numerous hubs inconvenience. IDS will follow the appropriated underlying model, which accumulates the comparative IDS clients, works in each hub of the organization. After this IDS clients to speak with each other to achieve the objective or for an interruption occasion. Each id usefulness is portrayed as follows:

DOI: 10.15680/IJIRCCE.2019. 0710010

Network Monitoring: Every IDS client acutely watches the organization and gets and administer individual information passing from the prompt neighbor in all actuality.

Interruption Detection: Every IDS client follows a particular based way to deal with identify assaults, i.e., it distinguishes the distinction in conduct of the hubs in view of the client decided rules. The organization managers need to decide and soak in the spot the powerful outcome for each assault that the IDS have dared to distinguish. The standard for the assault is remarkable, and are depicted in the impending segments:

Independent direction: Due to the partially blind perspective on the area, a hub can't go with a definite choice, whether that hub is totally an interloper. That organization wouldn't be reliable, on the grounds that it very well might be a venomous organization. In the event that something uncommon is distinguished by an IDS client, the brought together system is given the adjoining hubs. Consequently they can reach a typical resolution.

Activity: Each hub has a response component that will answer an interruption state. .

As per these capabilities, design is worked for IDS client utilizing five theoretical modules, as displayed in Figure 3. Each module has its own particular obligation, as displayed in the image. The IDS clients are comparative in hubs, thus they can impart the data to clients in the neighbor hubs. Consider the sinkhole assault situation, BS will supervise whole hubs in the organization and assembles the information in regards to the thought hubs. The assembled data is sent to different hubs through BS.

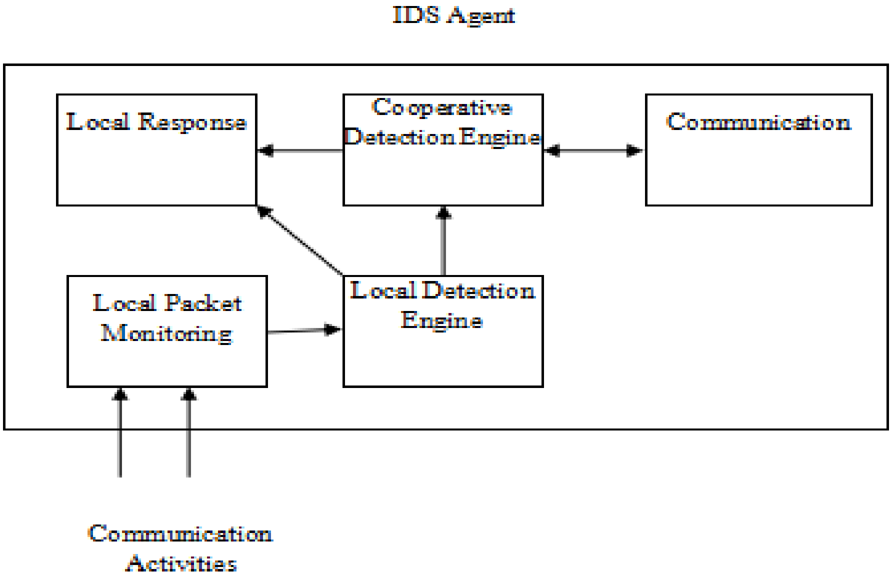


Figure 3: Structure of IDS

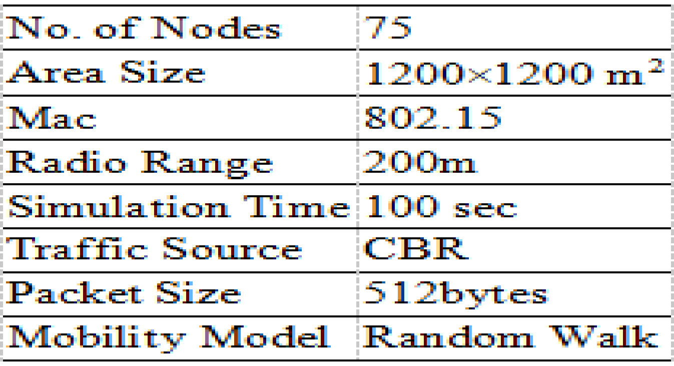
3.5. Artificial Bee Genetic Colony for QoS multicast Routing Problem

The Artificial Genetic Bee Colony Algorithm is used to give an answer for QoS multicast Routing Problem. Design the populace by choosing the arbitrary worth by the inquiry space, then, at that point, the arrangement vector is utilized to associate each person and its qualities are processed.

VI. RESULT AND DISCUSSION

In this examination work, comparison analysis of the current exploration systems are finished in the matlab tool. The network boundaries that are viewed as in this exploration work are displayed in the accompanying table 1.

Table 1. Simulation settings and parameters



No. of Nodes	75
Area Size	$1200\times1200\ m^2$
Mac	802.15
Radio Range	200m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	512bytes
Mobility Model	Random Walk

The simulation deployment outcome which is done based on parameter values given in the table 1 is shown in the following figure 4.

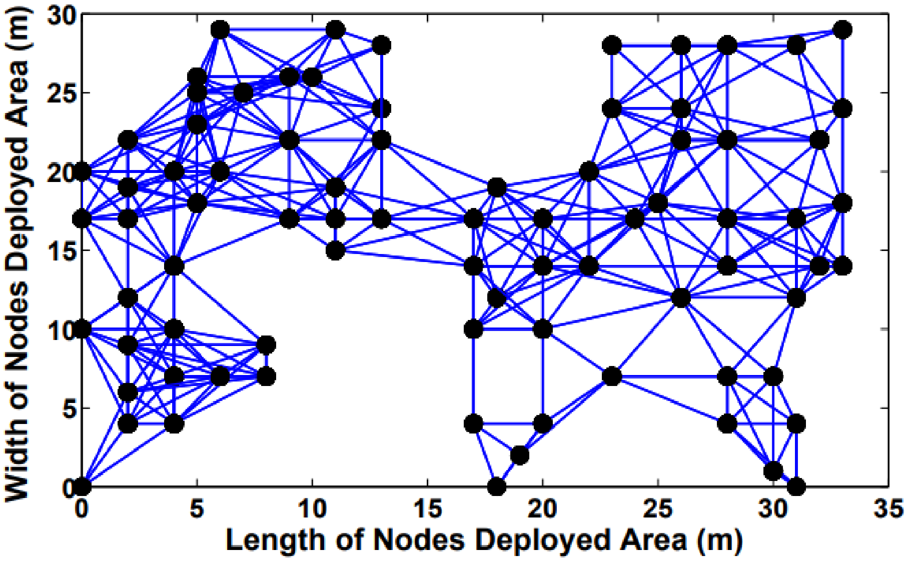


Figure 4: Deployment of Real field sensor nodes over the area of 1200 x 1200m, links are shown in blue line and black dot is the sensor node

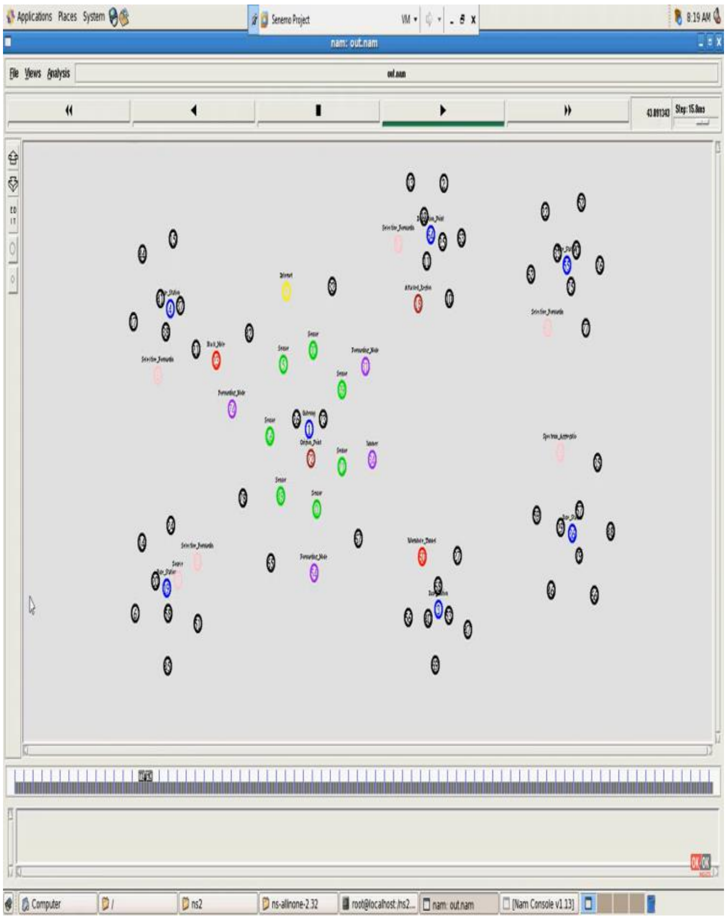


Figure 5. Wireless sensor network environment

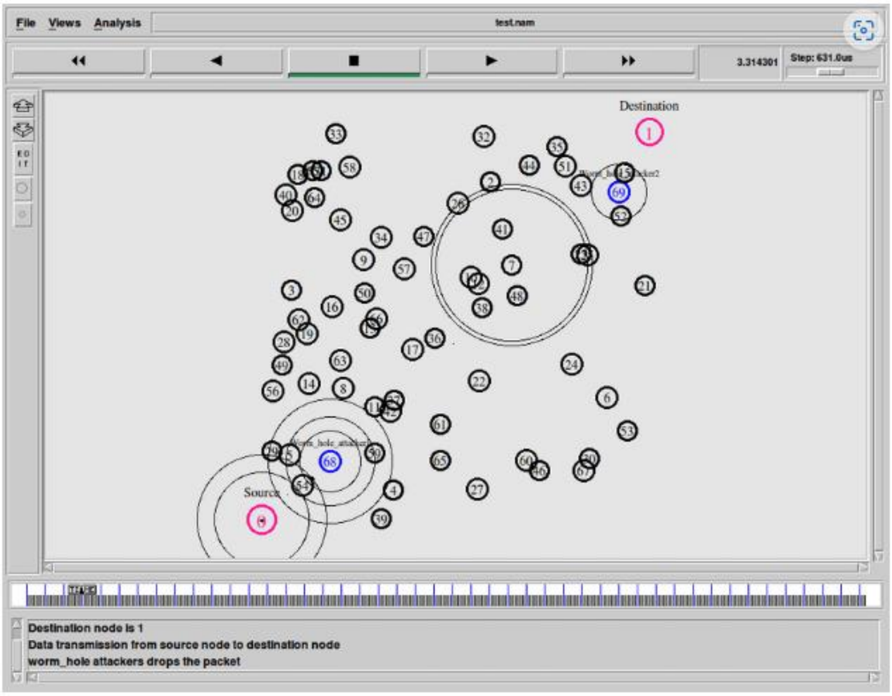
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 10, October 2019



Destination node is 1
Data transmission from source node to destination node
worm_hole attackers drops the packet

Figure 6. Network simulation in the presence of attack

In this work, comparison evaluation is done between the previous methodologies Route Reliability Ranking (RRR) algorithm, Fast ReRoute (FRR) Technique, Detection and Mitigation System (DMS) and the proposed Secured Energy Efficient Attack Mitigation System (SEEAMS).

Performance Evaluation

End-to-end delay: The average time taken by a packet to get transmitted from a source to a destination in a network.

$$End - to - end\ delay = \frac{\sum_{i=1}^{n}(t_{ri} - t_{si})}{n}$$

Where t_{ri} – ith packet receipt time, t_{si} – time the ith packet was sent and n - total packets.

DOI: 10.15680/IJIRCCE.2019. 0710010

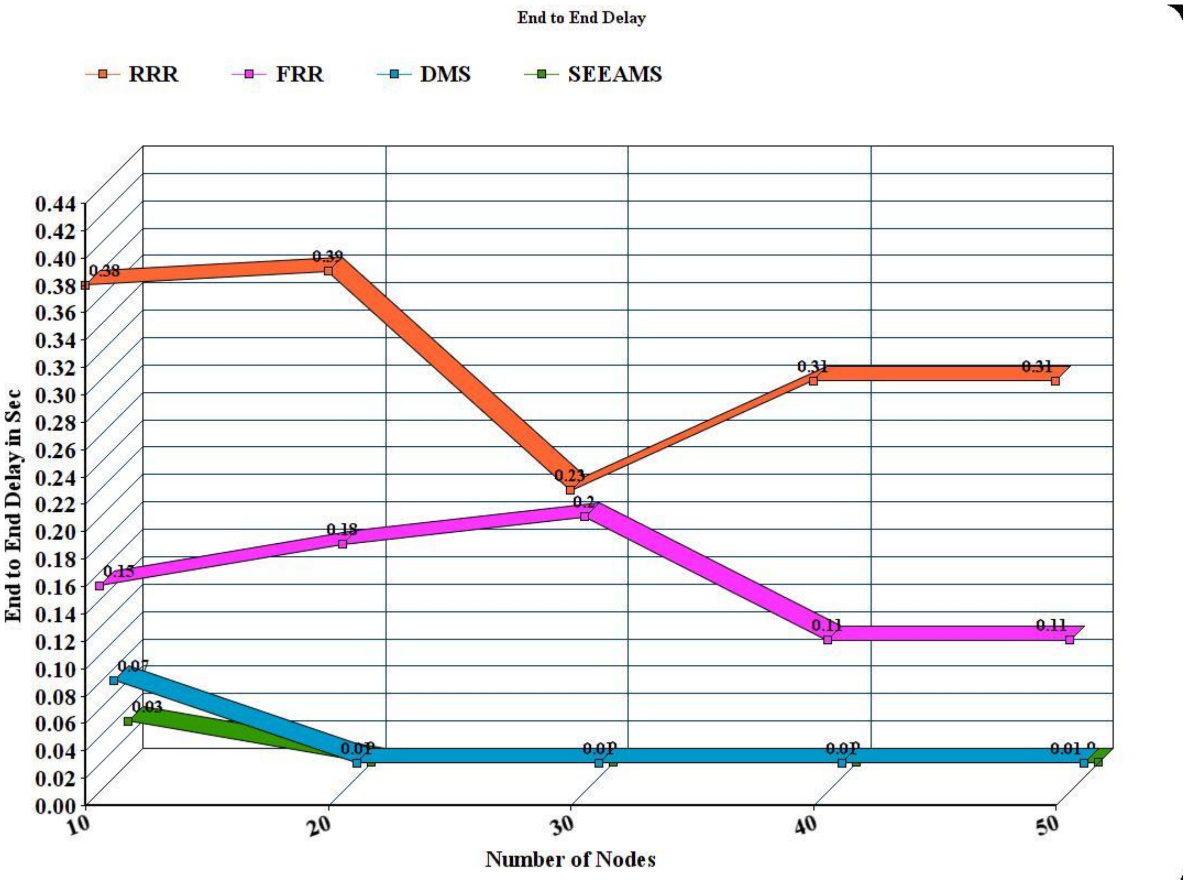


Figure 7. End-to-end delay comparison

Figure 7 portrays assessment examinations with regards to E2D execution
, where nodes are in x axisand y-pivot addresses their E2D values. Techniques analyzed are RRR, FRR, DMS and proposed SEEAMS calculation which shows lesser E2D. From the examination assessment, it is affirmed that the proposed SEEAMS accomplishes 72.72% lesser E2D than the DMS, 96% lesser E2D than FRR and 97.98% lesser E2D than the RRR.

Throughput: The rate wherein the packets are effectively communicated over the organization.

$$Throughput = total\ number\ of\ packets\ sent\ /time$$

DOI: 10.15680/IJIRCCE.2019. 0710010

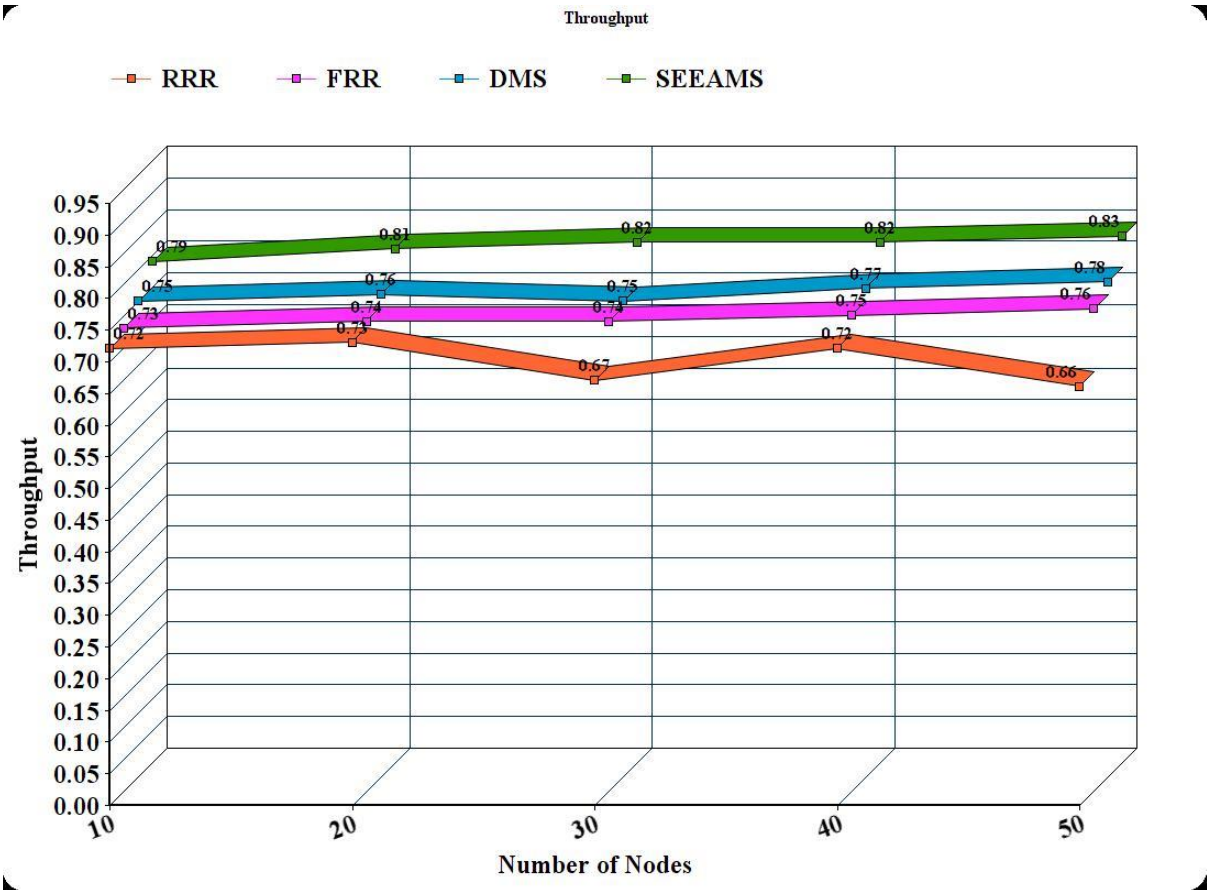


Figure 8. Throughput comparison

Figure 8 portrays assessment correlations regarding throughput execution, where nodes are in x-axis and y-axis addresses their throughput values. Strategies thought about are RRR, FRR, DMS and proposed SEEAMS calculation which shows higher throughput. From the graphical correlation it is affirmed that the proposed SEEAMS achieves 6.82% expanded throughput than DMS, 9.4% expanded throughput than FRR and 16.28% expanded throughput than RRR.

Energy utilization: Energy utilization is the typical energy essential for transmission of a packet to a node in the organization in a particular timeframe

$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d$

Where pi - data packet, e_t - packet i's transmission energy, e_r - energy required for receiving packet I and d - distance between transmission and destination nodes.

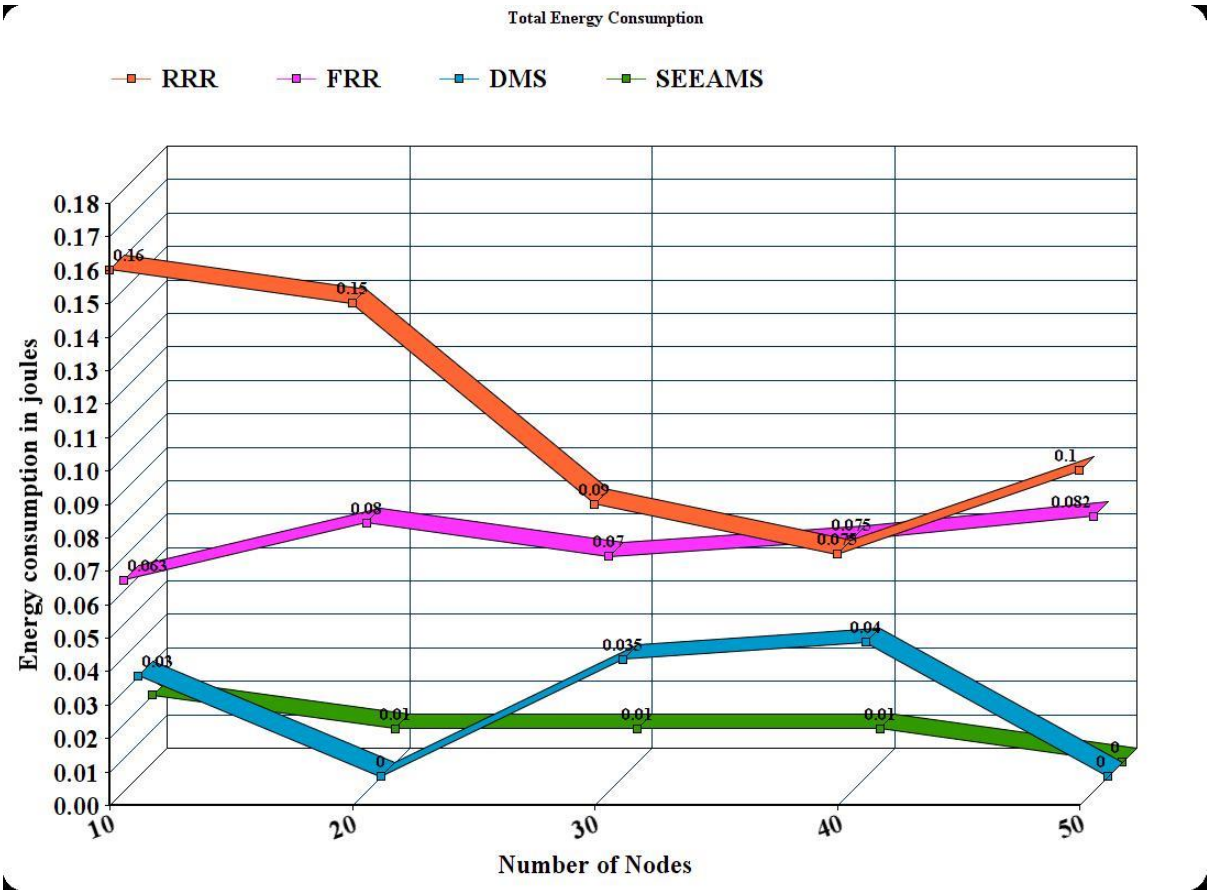


Figure 9. Energy utilization examination

Figure 9 portrays assessment examinations with regards to energy utilization execution, where nodes are in x-pivot and y-axis addresses their energy utilization values. Strategies analyzed are RRR, FRR, DMS and proposed calculation SEEAMS which shows lower energy utilization. From the correlation assessment, it is affirmed that the proposed technique SEEAMS achieves 52.38% lesser energy utilization than DMS, 86.48% lesser energy utilization than FRR and 91.3% lesser energy utilization than RRR.

Network lifetime : The lifetime of an organization.

$$Lifetime\ \mathbb{E}[L] = \frac{\varepsilon_0 - \mathbb{E}[E_w]}{P + \lambda \mathbb{E}[E_r]}$$

Where P - constant power consumption of network and continuous, ε_0 - total non-rechargeable initial energy, λ - average sensor reporting rate, $\mathbb{E}[E_w]$ – anticipated wasted energy or unused energy till the network dies and $\mathbb{E}[E_r]$ – reported energy consumption of nodes.

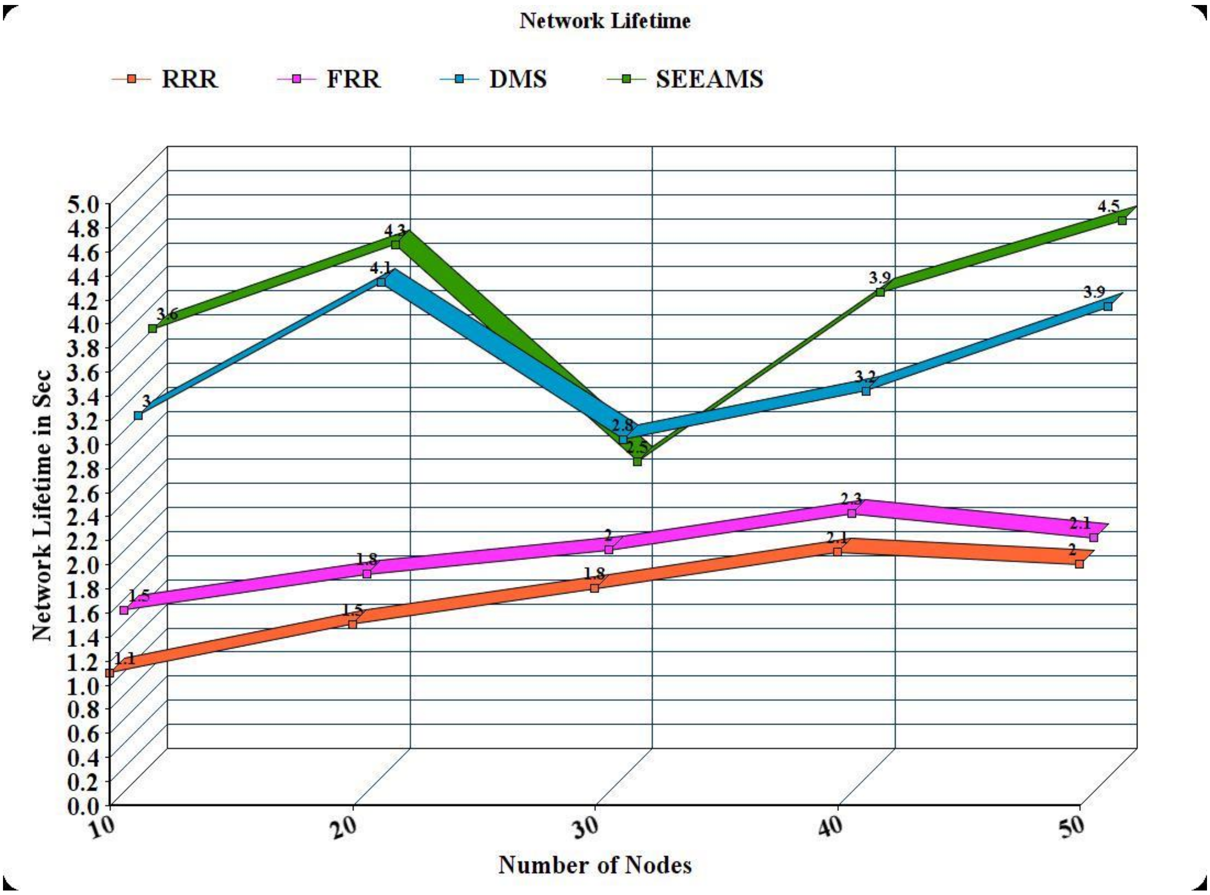


Figure 10. Network lifetime

Figure 10 portrays assessment examinations with regards to organize lifetime execution, where nodes are in x-pivot and y-axis addresses their organization lifetime values. Techniques thought about are RRR, FRR, DMS and proposed SEEAMS calculation which shows higher organization lifetime. From the graphical examination, it is affirmed that the proposed SEEAMS accomplishes 10.58% higher organization lifetime than DMS, 93.81% higher organization lifetime than FRR, 121.17% higher organization lifetime than RRR.

PDR: addresses the proportion of the quantity of lost packets to the complete number of sent packets

Packet loss ratio $=\frac{N^{tx}-N^{rx}}{N^{tx}} \times 100\%$

Where N^{tx} - transmitted packets, N^{rx} - received packets. This evaluation was done by extracting all real-time packet sizes that were transmitted and received.

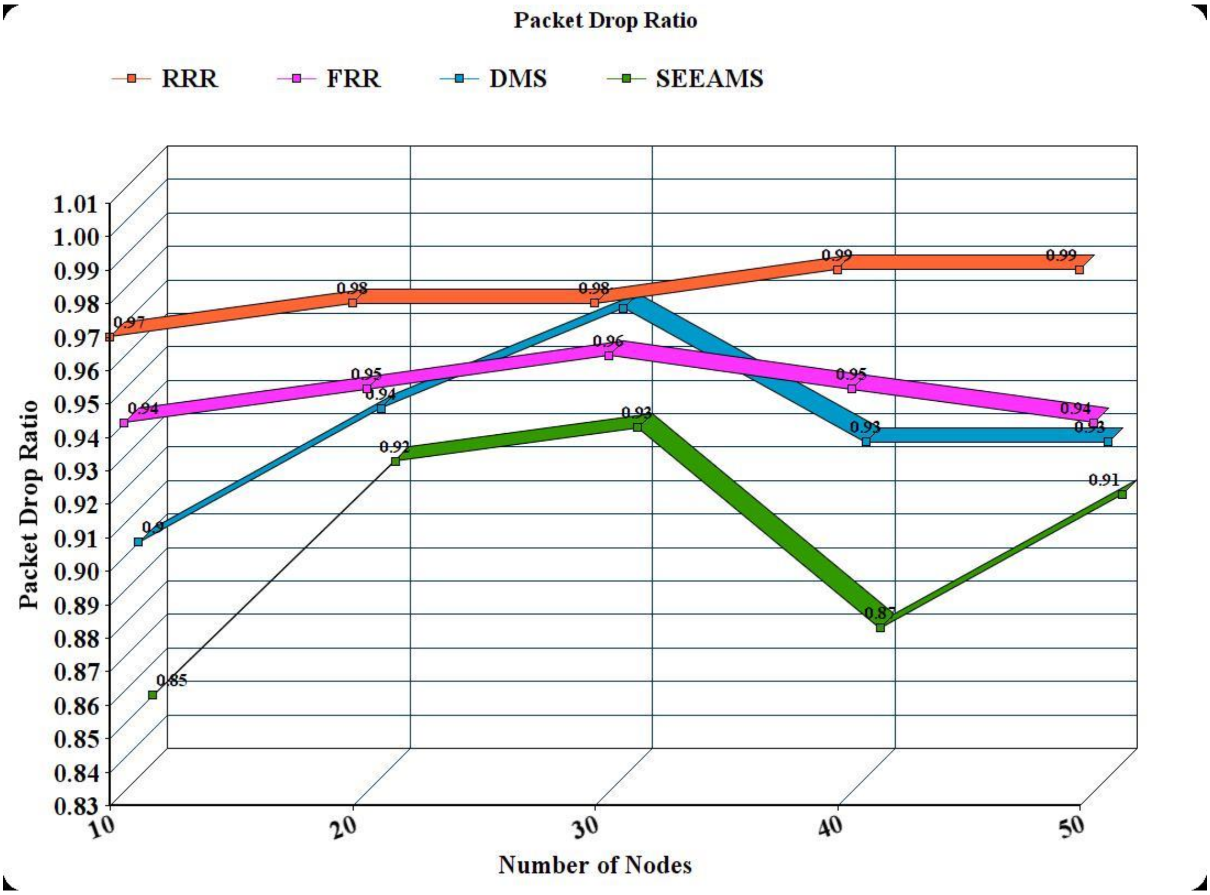


Figure 11. Packet drop proportion

Figure 11 portrays assessment correlations regarding PDR execution, where hubs are in x-pivot and y-hub addresses their PDR values. Strategies looked at are RRR, FRR, DMS and proposed SEEAMS calculation which shows lower PDR. From the correlation assessment, it is affirmed that the proposed technique SEEAMS achieves 4.06% diminished packet drop proportion than DMS, 5.48% diminished packet drop proportion than FRR and 8.75% diminished packet drop proportion than RRR.

V. CONCLUSION

In this research work, initial route path establishment is done using dijkstrakth shortest path algorithm. Once the population is initialized fitness value will be evaluated for each population of route paths. Based on calculated fitness value of each route path, route choice probability will be calculated. The route path with maximum probability will be elected for the optimal data transmission. To ensure the optimal route path selection, this work adapted the Hybrid Artificial Bee Genetic Colony based route path selection. To secure the data transmission from the malicious attacks, in this work Intrusion Detection System is integrated in the sensor nodes which will monitor and predict the malicious patterns occurring on the data’s that are transmitted. The general assessment of the examination work is finished in the NS2 tool from which it is demonstrated that the proposed research work achieves preferred execution over the existing exploration techniques.

REFERENCES

1. Abdulkarem, M., Samsudin, K., Rokhani, F. Z., & A Rasid, M. F. (2020). Wireless sensor network for structural health monitoring: a contemporary review of technologies, challenges, and future direction. *Structural Health Monitoring*, *19*(3), 693-735.
2. Gupta, J., Kathuria, A., & Sengupta, J. (2018). Secure and Energy Efficient Routing in Wireless Multihop Clustered Networks Based on RSSI.
3. Saha, H. N., Roy, R., Chakraborty, M., & Sarkar, C. (2021). IoT-enabled agricultural system application, challenges and security issues. *Agricultural informatics: automation using the iot and machine learning*, 223-247.
4. Lv, Z., Hu, B., & Lv, H. (2019). Infrastructure monitoring and operation for smart cities based on IoT system. *IEEE Transactions on Industrial Informatics*, *16*(3), 1957-1962.
5. Renold, A. P., & Ganesh, A. B. (2019). Energy efficient secure data collection with path-constrained mobile sink in duty-cycled unattended wireless sensor network. *Pervasive and Mobile Computing*, *55*, 1-12.
6. Ramadan, K. F., Dessouky, M. I., Abd-Elnaby, M., & Abd El-Samie, F. E. (2018). Node-power-based MAC protocol with adaptive listening period for wireless sensor networks. *AEU-International Journal of Electronics and Communications*, *84*, 46-56.
7. Fu, X., & Yang, Y. (2020). Modeling and analysis of cascading node-link failures in multi-sink wireless sensor networks. *Reliability Engineering & System Safety*, *197*, 106815.
8. Foundaion, K. L. E. Secure Energy Efficient Attack Resilient Routing Technique for Zone based Wireless Sensor Network.
9. Raj, J. S., & Basar, A. (2019). QoS optimization of energy efficient routing in IoT wireless sensor networks. *Journal of ISMAC*, *1*(01), 12-23.
10. Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems*, *79*, 103278.
11. Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly reliable and low-complexity image compression scheme using neighborhood correlation sequence algorithm in WSN. *IEEE Transactions on Reliability*, *69*(4), 1398-1423.
12. Karthick, S. (2018). TDP: A novel secure and energy aware routing protocol for wireless sensor networks. *International Journal of Intelligent Engineering and Systems*, *11*(2), 76-84.
13. Abdel Hakeem, S. A., Hady, A. A., & Kim, H. (2019). RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis. *Electronics*, *8*(2), 186.
14. Mukherjee, A. (2018). Energy efficiency and delay in 5G ultra-reliable low-latency communications system architectures. *IEEE network*, *32*(2), 55-61.
15. Santhosh Kumar, S. V. N., & Palanichamy, Y. (2018). Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN. *Wireless Networks*, *24*(4), 1343-1360.
16. Prithi, S., & Sumathi, S. (2020). LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network. *Ad Hoc Networks*, *97*, 102024.
17. Thangaramya, K., Kulothungan, K., Indira Gandhi, S., Selvi, M., Santhosh Kumar, S. V. N., & Arputharaj, K. (2020). Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. *Soft Computing*, *24*(21), 16483-16497.
18. Selvakumar, K., Sairamesh, L., & Kannan, A. (2017). An intelligent energy aware secured algorithm for routing in wireless sensor networks. *Wireless Personal Communications*, *96*(3), 4781-4798.
19. Haseeb, K., Ud Din, I., Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors*, *20*(7), 2081.
20. Haseeb, K., Almogren, A., Islam, N., Ud Din, I., & Jan, Z. (2019). An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. *Energies*, *12*(21), 4174.
21. Sarkar, A., & Senthil Murugan, T. (2019). Cluster head selection for energy efficient and delay-less routing in wireless sensor network. *Wireless Networks*, *25*(1), 303-320.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 10, October 2019

22. Srivastava, V., Tripathi, S., Singh, K., & Son, L. H. (2020). Energy efficient optimized rate based congestion control routing in wireless sensor network. *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1325-1338.
23. Sajwan, M., Gosain, D., & Sharma, A. K. (2018). Hybrid energy-efficient multi-path routing for wireless sensor networks. *Computers & Electrical Engineering*, *67*, 96-113.
24. Dhand, G., & Tyagi, S. S. (2019). SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. *Wireless Personal Communications*, *105*(1), 17-35.
25. Nalinipriya, **K.G. Maheswari**, Balamurugan Balusamy , K. Kotteswari and Arun Kumar Sangaiah , "Availability modeling for multi-tier cloud environment" **IntellIgent AutomAtIon & Soft ComputIng,** Vol. 23, no. 3, PP. 485–492, ISSN: 1079-8587, 2017.
26. G. Nalinipriya, P.J.Varalakshmi, K.G.Maheswari, R. Anita, 'An Extensive Survey on Co- Resident Attack in Dynamic Cloud Computing Environment" published in **International Journal of Applied Engineering Research ,** ISSN 0973-4562 , Volume 11, Number 5 , pp 3019-3023 , **2016.**