**ENHANCED FIREFLY OPTIMIZATION ALGORITHM WITH IMPROVED FAULT-TOLERANCE FOR MALWARE DETECTION OVER IOT BASED WSN**

Udaya Suriya Rajkumar D1\*, Shanmugaraja P2, Sathiyaraj R3, Mohan D4, S. Kerthy5

1\*Professor, Department of Computer Science and Engineering, GLOBAL Institute of Engineering and Technology, Ranipet, Tamil Nadu, India. Email: u\_suriya@yahoo.com

2Associate Professor, Department of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India. Email: [shanmugarajap@gmail.com](mailto:shanmugarajap@gmail.com)

3Assistant Professor, Department of CSE, GITAM School of Technology, GITAM University, Bangalore, Karnataka, India, Email: rsr026@gmail.com

4Assistant Professor, Department of Computer Science and Engineering, Global Institute of Engineering and Technology, Melvisharam, Tamil Nadu, India.

Email: [dm.mohan14@gmail.com](mailto:dm.mohan14@gmail.com)

5Assistant Professor, Department of Information Technology, Jeppiaar Institute of Technology, Kunnam, Chennai, Tamil Nadu, India. Email: skerthyit@gmail.com

\*All correspondence shall be communicated to Udaya Suriya Rajkumar D ([u\_suriya@yahoo.com](mailto:u_suriya@yahoo.com))

**Abstract**

Wireless Sensor Networks (WSNs) have gained recognition and reputation in view of their use for various purposes. When a WSN is used for a crucial Internet of Things (IoT) application, evaluation of the dependability of the deployment is a job that is of utmost importance. Still, the existing system has problems with lower packet delivery ratio since inappropriate Cluster Head (CH) selection process. Also, the shortest path routing and malware detection performance is poor and, as a result, the total IoT-based WSN performance suffers greatly. In this study, the Enhanced Fire Fly (EFF) and Fault tolerance based Ad-hoc on demand Distance Vector Routing (FAODV) protocol is offered as a resolution to the problems seen in the focus on optimal, faster and energy efficient data transmission assuming the shortest path routing based fault tolerance and malware attack detection performance. System modelling, choice of CH nodes, and the shortest route and virus detection are among the major steps of this effort. Initially, the system model is constructed a with certain number of nodes in IoT based WSN. Then, using the EFF method, the best CH node selection is carried out for acceleration of data transfer as well as energy efficiency through use of the best fitness function values. The Shortest path routing is done using AODV protocol. Also, fault tolerance mechanism is applied for handling the route or node failure and providing continuous services through another route. The FOADV protocol is utilized for the effective removal of the malware attack nodes. FAODV protocol is used for increase in the security level for fast data transmission over IoT based WSN. The simulation findings indicate the out performance of proposed EFF-FAODV framework over the previous techniques in terms of throughput, network lifespan, higher packet delivery ratio, and lower energy usage as well as end-to-end latency. The efficiency of the overall IoT based WSN is 91% which is better than that of any of the earlier methods.

**Key words:** Cluster Head, Energy Efficient, Enhanced FireFly (EFF), Internet of Things, Malware detection, Wireless Sensor Network, .

1. **Introduction**

The rapid growth of the internet of things has led to the utilization of WSN in a variety of areas, including industrial automated control, environmental monitoring, and smart home systems. WSN has a broad scope of application in the diverse functioning field and furthermore well matched for long-standing information attainment. It is also with inclusion of the top sensor interfacing mechanism in the IoT setting [1]. Distributed sensors known for background constraints such as heat, stress, noise, etc. and exceeds their sensed data via the route to the central positions. These pathways are built through routing which is a procedure for the creation of a route among a source node and a destination node from an existing path. The cluster-based routing mechanism illustrates improved power consumption ratio than the non-cluster routing method [2].

Cluster-based techniques employ certain nodes as CH prior to transmission to a sink,to enable optimal organization of WSN’s for data aggregation and utilization of energy. A CH transmits data that has been compiled or compressed by cluster nodes [3]. But with the node having additional tasks, the network suffers irregular degradation due to a larger energy drain. It chooses a CH for assembling to assemble sensed data from the CH around the goal for facilitating data aggregation . Aggregation of the sensed data near to the data source could be taken up for elimination of extensive distance data and expensive collection of lower data. Additionally, in the effective target tracking strategy, every CH has a changing lifespan based on its position and left-over energy to balance the energy cost.

A majority of WSN applications need continuous monitoring; therefore, this is another crucial requirement. As a result, issues relating to these longevity and coverage of the networks are significant due to the high dependence WSN performance is on the life time of the network. So, while building WSNs with extended life spans, energy saving is a severe and vital concern. With careful management of energy resources, energy conservation becomes feasible knowledge of the most energy-intensive components of WSNs is the first step in reducing their energy use. This information is crucial for the selection of the best strategy. Compared to the compute subsystem, the communication subsystem uses a lot more energy. A piece of data sent uses the same amount of energy as for the execution of a few thousand instruction. This is shown [4-5]. As a result, jobs involving processing and communication require balancing. While radio energy consumption is the same for all modes of operation reception, transmission, and idleness it decreases by at least a factor of two while the device is in sleep mode. In light of this, it makes sense to mute the radio for as long as we can. A significant amount of energy consumption, depending on the application, may come from the sensory subsystem.

WSN application is being constrained by security issues. Attack refers to an intentional effort to deny a legitimate user of a service access. Attacks have been the key concern and problem for the security of WSN due to the restricted supply of sensor nodes [6]. Denial of Service (DoS), Jamming, Node destruction, Spoofing, replaying, denial of sleep, Sybil assaults, and Distributed DoS are just a few examples of the many types of attacks that may occur in WSN. The routing protocol of WSN is susceptible to DoS attacks due to a majority of its routing methods being straightforward and effective. The architecture of the networks, however, depends on the routing protocol. Network configuration gets disturbed and the network performance significantly impacted when the routing protocol is assaulted by a routing layer flood attack.

The objective of this paper is to explain the use of sensor nodes in WSN to ensure safe data delivery. The development of numerous research initiatives and methodologies has produced only a little advancement in the detection of malware attacks. Energy usage and shortest route routing are problems with the current methods in WSN. This study proposes the EFF+FAODV protocol for improvement of the complete task of the WSN system for then purpose of addressing the aforementioned problems. The primary contributions of this investigations include an IoT-based WSN model, the use of the FAODV protocol for the shortest route routing, and the selection of CH nodes using the EFF algorithm. With the utilization of efficient techniques for the WSN, the suggested solution aims at increase in network lifespan while reducing energy usage.

The remaining sections are arranged as : Section 2, deals with a work of the research related to WSN of fault tolerance, attack detection, and CH selection. Section 3 provides additional information on the given technique for the EFF+FAODV protocol. Section 4 contains the performance study discussion and simulation results. Section 5,provides a summary of the results.

1. **Related work**

In [7], the author has presented a firefly algorithm in WSNs for collection of data. The approach uses clustering for separation the sensor nodes into several regions with Nodes cycle in and out of activity in each cluster. The selection of active nodes takes into account factors such as energy and distance. This enables the choice of active nodes from nodes with higher energy left and greater distance. In cluster based WSNs, CHs require additional energy due to aggregation of data from cluster associate nodes and movement of the aggregated data to the sink. As a result, one of the key elements in the decision of the longevity of wireless sensor networks will remain operational lies in making the right choice of CHs. Based on the findings of the simulations, the approach gets the ability to improve quality of service parameters more than other algorithms currently in use.

In [8], created a cutting-edge IoT botnet propagation model that was centred on IoT networks. Their investigation related to the effect of IoT exact issue on botnet development. Examination of the connections among node power, network density, attack surface size and scanning behaviour size for various scanning techniques, helped getting capability to improve knowledge of the botnet threat to sensor nodes. The simulations demonstrated the ineffectiveness of violent propagation strategies in the acquisition of nodes and the provision of superior activity distribution, by dense networks ensuring life time for individual bots. There was also the demonstration of a significant improvement in the probability of scanning rates and broadcast the focus of future models will be focus on a few key IOT exact phenomena, such as the express energy exhaustion of sink nodes, the utilize of encryption and the consequence of mobility.

WSN is critical to a number of sectors, including the military, healthcare and information technology like the Internet of Things, as highlighted in [9]. In the absence of any construct in safety mechanism fixed in the IoT device, WSN has a drawback in its application due to the limitations seen of the sensor nodes in conditions of memory, CPU and battery. As an outcome WSN is susceptible to attacks one of which that frequently occurs being the DOS attack. These attacks strive to avoid legitimate users from utilizing resources by decrease in available resources until the network resources get overloaded, and the network turns into sluggish and eventually the network falls off. Identification and reduction in DoS risks is for stopping these attacks using a jamming tactic on the attacking node. Recognition and mitigation of DoS threat are requested for halting the threat. The method utilized in this work for detection and mitigation of Dos attack utilize a signature-based Intrusion Detection System, which deploys a jamming strategy on the attack node and blocks all packets coming from the attacker till the attacker running out of energy. The jamming method can be utilized as a improvement method for DoS attacks by stopping all packets originating from the attacker.

In [10], refer to the main issues with WSNs as a shorter network lifespan and data transmission delays. Data routing is particularly important in many key applications, including disaster management, environmental monitoring, and numerous military and other critical ones. However, it has been shown to be ineffective in Multi hop low energy adaptive clustering hierarchy protocol. NP-hardness exists in cluster head optimization. This article recommends the choice of the best routing option for the extension of the life of a network and increase its energy efficiency. Despite the presence of a poor local optima issue, a variety of meta-heuristic approaches, including PSO, have been employed successfully based on PSO and Tabu search algorithms, the technique, with increase in the amount of clusters created, the percentage of nodes that are still active, and by lowering the packet loss rate and the end to end, the results demonstrate the effectiveness of the Tabu PSO.

In [11], the resource-constrained, remotely deployed sensor nodes in WSN are dispersed in nature. The security of data transmission is compromised due to their susceptibility to several threats. One of the most common assaults that jam the sensor nodes is the denial of service (DoS) attack. There are several methods available to stop sensor node jamming. A few of the methods are derived from cryptographic algorithms, which are notoriously difficult to put into practice. However, when the method is straightforward, it will be easy for the adversary to penetrate the environment in which it is deployed. As a result, an innovative method based on a clustering approach and timestamp is used. This method comprises two primary contributions. The first one is determined by the clustering of the sensor nodes, and the second by the timestamp that is computed from one node to another. The presence of malicious nodes is acknowledged when the timestamp exceeds the time boundary, and jamming is seen when the signature doesn't match and the acknowledgment is decrypted. Following this, the broadcast is stopped and redistributed through a different channel. The Packet Delivery Ratio (PDR), Network throughput, Energy used, and Routing overhead are used to assess the performance measure, which shows the superiority of performance to the methods currently in use.

In [12], demonstrated how malware travels across the whole WSN through wireless connection starting with a hacked sensor node. A better mathematical model that combines quarantine and vaccination procedures was established as a result of malware quarantine. It was able to retrieve the model's equilibrium points and other key parameters. The system’s stability under various conditions was looked at utilizes the fundamental reproduction number to determine malware is still present in the system. It facilitates in the process of figuring out the communication radius and the node density cut off limit. In this model, the influence of a number of different factors is investigated. In terms of lowering the pace at which malware is spread and cutting down on the number of infected nodes, the performance has been seen to be greatly improved in comparison to the previous models and has been confirmed by comprehensive simulation results.

In [13], aims to comprehension of the many fault kinds that may arise in a WSN. Enhancement of the resilience and self-healing capabilities of the sensor network the main goal of the fault-tolerant approach. Different forms of WSN failures are typically attracted by the resource-constrained environment, distant deployment, and difficult monitoring settings. Two methods, including fault tolerance and fault preventive methods, are available for handling the problem. The existing methods, have a problem with early identification of attacks for the effective conclusion and better results, as also with optimized CH node selection leading to lower performance, along with problems along with energy consumption and shortest path routing process. The existing system has not provided effective attack detection and hence it affects the efficiency of IoT based WSN. Robust CH node selection, with FAODV algorithm is considered for accurate detection of the attacks from the IoT based WSN. The proposed work also involves the use of EFF algorithm for a significant increase in energy efficiency.

In [23] examines the impact of tolerance for failure on the mechanism through introducing fake issues into the router approach on the system prior to removing them. An significant improvement happened whenever a router on a synchronized network assessed the buffering capacity of network tolerance for faults by introducing error to the buffer. A way to enhance fault tolerance has been suggested and it effectively makes use of the resources that are accessible. The Support Vector Machine algorithm and Harris Hawks Optimization (HHO) algorithm make up the suggested technique in [24]. The HHO algorithm function is to optimize the hyper parameters of the SVM classifier, allowing the SVM to classify malware according to the best selected method and to generate the optimum features weighting solution. In [25] fusion of deep learning supported cyber attack identification and classification methods for intelligent systems called FDL-CADIS approach. The suggested method converts the Malicious binary files into two-dimensional images, which the fusion method subsequently classifies. In order to extract features from the the binary input images, the MobileNetv2 method is used in the technique. The black widow optimize method is then used to tune the hyper parameter.

This section discusses the various authors’ research work in the examination of the different techniques involved in the detection of attacks. Many studies relate to the enhancement of detection accuracy in a variety of ways. Malware detection system using CH node selection, energy efficiency and routing process has been developed. The steps included are examined in different authors perceptive to get the better knowledge about particular steps. Along with this introduced and discussed techniques more helpful in the analysis of malware detection with accurate and minimum time. Additionally, a thorough description of the techniques that have been created, their characteristics, and performance metrics has been provided. Each technique has its own drawbacks benefits, and the outcomes have been addressed.

1. **Proposed methodology**

In this work, Enhanced FireFly (EFF) algorithm and Fault Tolerance Ad-hoc on demand Distance Vector Routing (FAODV) protocol have been proposed for efficient malware detection over IoT based WSN. The system model of the work is its primary contribution, CH node selection using EFF and fault tolerance based attack detection using FAODV protocol.

* 1. **IoT based WSN system model**

This work, is based on the assumption of every IoT-based WSN node as in a vulnerable condition at this start of this sensor network. Meaning that although they are malware-free, they are nonetheless open to threats. Take into account a network with a total of node, where Consequently, it is expected that the node population would stay constant: each successive moment. For a specific period, N represents the number of agents there, S(t) the agents who are prone, E(t) indicates how many agents have been exposed, I(t) shows the number of agents present in the infected condition, R(t) the agents that have been retrieved, and finally F(t) the agents in a failing state are indicated by this. Consequently, the best and the most effective defence against malware attacks comes from the combination of both, along with the latent duration concept [14]. The longevity of IoT-based WSN is increased by this approach.

Each of the proposed nodes of the model has six separate states:

1. Vulnerable nodes (S): IoT based sensor network nodes that are susceptible to malware assaults. The sensor has the potential to fail or get infected but is functioning well without any subsystem breakdown and without malware infection.
2. Exposed nodes (E): Malware-infected network nodes that do not infect their neighbours. The built-in malware detection and removal system of the nodes are included.
3. Infectious nodes (I): Network nodes that have experienced a malware assault and are capable of infecting nearby nodes.
4. Recovered nodes (R): Sensor nodes in the network that have improved from an illness or have had infections removed from them.
5. Failed: The sensor that malfunctions as a result of malicious physical damage, subsystem malfunction, running out of battery life, or fast drain when malware is present.

**Agents and environmental characteristics**

The primary component of WSN is the data that sensors can gather from the environment. The following sensor qualities based on dependability and security are taken into account:

* Reliability state of sensor: The ordinary state and the failure state are the two states that the sensor may be in. In a typical condition, the sensor is capable of performing the anticipated tasks such as data collection, processing, and transmission. One or more of these functions cannot be carried out while the system is in the failure state.
* Reliability level: corresponding to sensor nodes with dependability levels ranging from high to low, the sensor has been separated into a high level, medium level, and low level.
* Security level: has been ranked as having a high degree of security when the most tried-and-true precautions have been taken, a medium level of security when just the most fundamental precautions have been taken, and a poor level of security when no security measures have been taken at all.
* Transmission capability: Certain nodes are prevented from infecting their neighbours with the use of software and hardware functions, and as a result, they cannot transmit malware.
* Battery power: fundamentally plays a responsibility in determining the lifespan of the sensor node and, thus, its dependability [15]. The initial power provided by the battery may be broken down into three distinct categories, ranging from low to high.

Any software that is maliciously created with the express reason of cause harm to a computer, server, client or network. Malware is taken into account in the model for the following two traits:

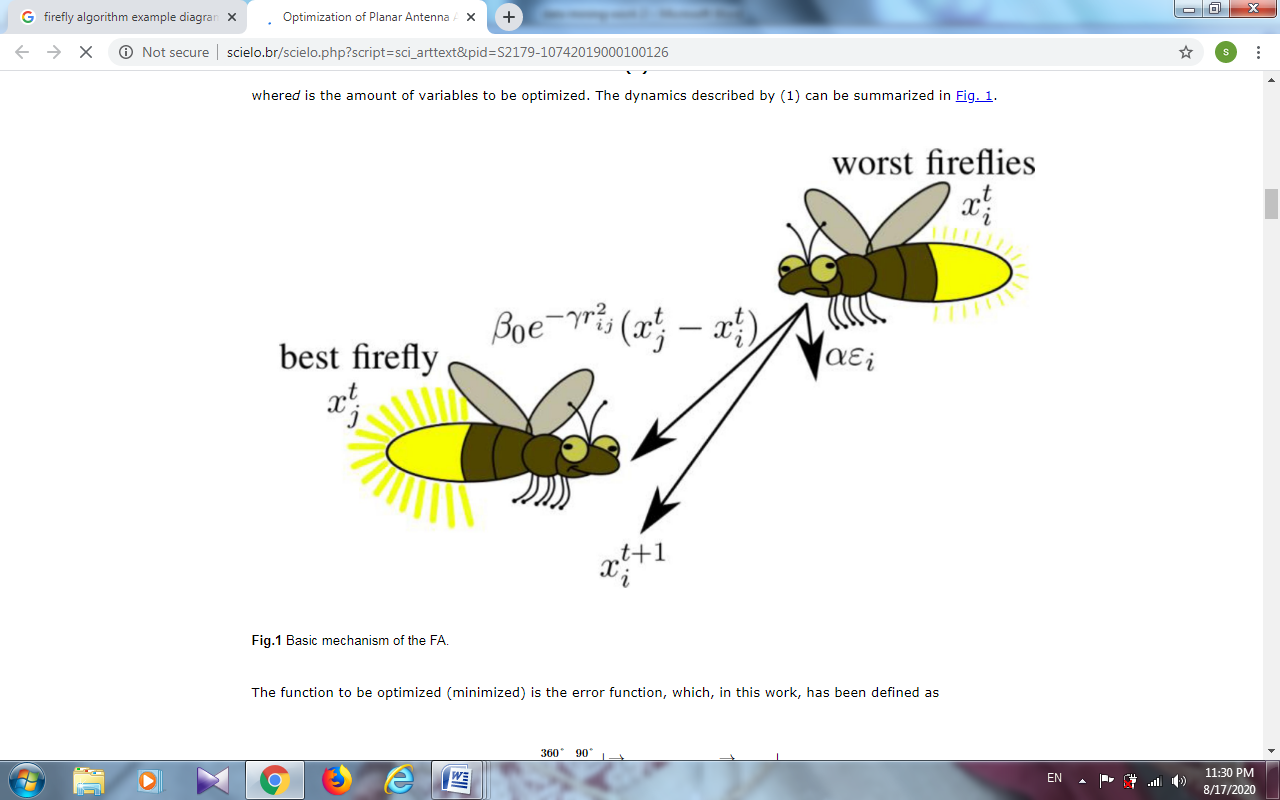
Malware assault power is measured by infection intensity, and malware with higher infection intensities has a larger likelihood of infecting nearby nodes. A very high or extremely low infection intensity is possible.

Target: Malware is made for a variety of goals; some are intended for interference with software performance, others for the use of more energy and use batteries more quickly, and yet others to harm hardware. The software function, the hardware of a subsystem, or the battery power might be the goal.

* 1. **Energy efficient based Cluster Head (CH) node selection using Enhanced FireFly (EFF) optimization algorithm in IoT based WSN**

In this study, choice of the best CH is accomplished with the use of Enhanced FireFly (EFF) algorithm for energy efficiency. Here fitness values considered are lower energy consumption and delay. CH gets dynamically updated for each period of time to ensure its on going offer with the necessary energy level. The main requirement of the CH selection model is that the CH, delay should be further away from the normal node than reduced whereas energy of the CH should be remains high.

The physiological and sociological characteristics of actual fireflies provide the basis for the Firefly algorithm [16]. Real fireflies emit a concise, rhythmic flash that acts as both a protective warning system and a means of attracting (communicating) their mating partners. The objective function of the concern that has to be optimized relates to the formulation of flashing behaviour. FA operates in a manner similar to how fireflies flash their lights. The firefly group shifts to intense and appealing spots as a result of the intensity, of light planned for the provision of the greatest resolution over the sought-after location. The firefly algorithm's primary mechanism is representing in Fig. 1



**Fig 1 Basic system of the firefly algorithm**

This mechanism normalizes few of the firefly features and can be shown as given below [17]:

1. Regardless of gender, every firefly is drawn to a separate person.
2. With the intensity a firefly creates openly related to its attractiveness, when there are two fireflies, the one with more brightness draws the one with less brightness. A firefly will randomly change course if it can’t find another firefly that is brighter nearby.

The brightness of the firefly has statistical influenced from by the objective method. The firefly method is chosen due to its ability to offer the best answer for multi-objective problems. For a maximizing trouble, the brightness might just be proportional to the objective function. To make things simple, it is assumed that attractiveness of a firefly is determined by its brightness or light intensity, which is correlated to the encoded goal function.

a) According to the inverse square rule light intensity fluctuates as follows: Light intensity and Attractiveness at the Source

(1)

Where I(r) is the light intensity at attractiveness

Attractive produced by random assignment for packet transmission

b) While the intermediate is offered, the light intensity is described as :

(2)

Where, represents the capacity of medium to absorbs energy.

c) The subsequent Gaussian approximation is taken in to account for keeping away from singularly.

(3)

On the basis of the degree of brightness of the surrounding fireflies seen, there is increase in the attractiveness of the firefly. A new solution is achieved on the consideration of this potential for variation and random modification of the allocation. Consequently a firefly's appeal consists of the following.

) (4)

Where is the attractiveness at r=0.

A batch of two fireflies (resources) are positioned I and j the following formula is used to calculate the distance between them:

(5)

Where is the kth a spatial match related factorof the kthd is the quantity of dimensions and firefly. For both absorption and random parameters, the Enhanced Firefly (EFF) optimization technique adds an adaptation parameter. These adjustments increase the capacity of local and global search through linear changes in the parameter during the iterations period [19].EFF is applied for producing the optimal CH nodes in network by performing best fitness values.

The following equation relates to the analysis of the parameter it goes behind:

(6)

The value is adjusted based on the extent of the optimization distance deviation for increase in the convergence speed and the accuracy of the solution. The sentence is simultaneously changed to provide a boost the population's adaptability in the manner described below.

(7)

Where (8)

are the maximum and minimum energy respectively. In Eq. (8), the lowest perform of generation in terms of position firefly, and is a measure of the distance of the distance of worst person from the ideal person overall. In the early phase of the algorithm, the firefly people are scattered throughout the whole area, with the mainstream of them situated far away from the people who are globally optimal. The significance of at this minute in occasion ∥∥ is larger, and () lies in constant values. As a result, it is greater in the early stages, featuring a significant impact on overall optimization, as explained by Eq. (7). When the technique is used, the particular firefly i is pulled to former, brighter fireflies that are near global optimum nodes. When the time comes, I'll collect the firefly people near the most ideal people i on the universe.∥ ∥is now smaller, which makes it easier to find the best nodes for WSN searches. The amount iteration of each α when the optimum is at its new location, this accelerates the algorithm's convergence speed. The step size factor, according to the study above α depending on how far apart the firefly individuals are from one another, which strikes a balance between the search and algorithm development capabilities.

A novel fitness function is assumed has been this study, along with energy consumption and delay that are determined by

(9)

Where the amount of mails that were not deliveredis the aggregate number of messages sent at a greater rate.

is the remaining power in node i.

is the initial power.

is the end-to-end delay and is the maximum allowable delay.

(10)

Where and between-firefly node distance

Each node in the population has its fitness value determined. The initial creation of networks makes random choice of the number of nodes to be present. The fitness value of each firefly is determined. Then, the selection process is utilized in the choice of two particular fireflies. Along with having a brighter brightness, the Firefly also has the highest fitness value, making it the choice for the next generation (CH selection)

**Algorithm 1: EFF for CH node selection**

Input: Number of sensor nodesand data packets

**Output:** Ensure Energy-efficiency

1. Start
2. Objective function (𝑥), 𝑥 = (𝑥1,...,)𝑇 consider lower energy consumption and delay as objective function
3. create the basic firefly population (nodes)S (𝑖 = )
4. Light intensity 𝐼𝑖 at 𝑥𝑖 is mentioned by 𝑓(𝑥𝑖)
5. Indicate the coefficient 𝛾 of light absorption
6. while (𝑡<MaxGeneration)
7. for 𝑖=1:𝑛 all 𝑛 fireflies
8. for 𝑗=1:𝑖 all 𝑛 fireflies
9. if (𝐼𝑗>𝐼𝑖), Move firefly 𝑖 in the direction 𝑗 in 𝑑-dimension;
10. end if
11. The CH neighbor sensor node requires identification.
12. With distance, attraction shifts𝑟 via exp[−𝛾𝑟]
13. Determine physical fitness using (9) and (10)
14. Create a model that is objective using (5)
15. Utilize updated light intensity estimates and novel ways to (2)
16. Reduce the overhead associated with data transfer by (10)
17. Utilizing, update the ideal CH node (7)
18. Improve the metrics for energy use and latency on the best neighbour CH sensor node.
19. end for 𝑗
20. end for 𝑖
21. Choose the current top fireflies by ranking them.
22. end while
23. Aggregates from high energy node
24. A firefly shifts to a additional attractive

According to Algorithm 1, the EFF algorithm is used to pick the CH nodes. The aggregated data from the CH is transmitted to the sink node in a particular hop as the final result of this procedure. Additional energy is required from the CH for data aggregation and data transmission to the sink node. The longevity of the network get reduced as outcomes of nodes failing in such scenario. This approach uses a periodic CHs voting mechanism for improvement of the over all effectiveness and prevention of the imbalance in energy use. A measurement of the residual energy and delay of the node is taken after each round in order to do this. Comparison is made to a predetermined threshold to ensure control over the aggregation and forward procedure. A new CH is selected in the event of a fall below the threshold, which affects how much energy each node needs. In turn, this increases data WSN efficiency and lengthens the network's lifetime. Using an improved energy and delay measure, the EFF algorithm generates the best possible solutions in this case. The best fireflies are selected using the greatest fitness values in the EFF algorithm, which ranks the fireflies.

* 1. **Shortest path routing and malware detection using Fault-tolerance based Ad-hoc on demand Distance Vector Routing (FAODV) protocol in IoT based WSN**

Improvement in the shortest path routing and malware detection over IoT based WSN with the introduction of the AODV algorithm are dealt with in this study. The suggested strategy avoids the requirement of rebroadcast messages from the source node in the event of a link failure. AODV routing method is used for carrying out the routing route in this section. It reduces transmission volume by establishing demand-driven channels. In situations when a source has to broadcast information, this protocol examines the route table [18]. The shortest routing route and the nodes with the best residual energy are chosen in the AODV algorithm throughout the assessment phase. It is used in the choice of the node that has the lowest amount of energy utilization, the least amount of latency, the highest network lifespan, and the highest throughput. Data packets are distributed across the produced pathways in a manner that is both effective and efficient.

The AODV protocol, which is based on the EFF, uses the best CH for the choice of the shortest path routing the enhanced metrics. In this case, node energy and multipath routing both show significant improvement . The major goal of this AODV protocol is to improve the performance of IoT-based WSNs by securing data transfer and leveraging route discovery and maintenance functions. The distance vector protocol known as AODV has a single route and uses a hop-by-hop routing method. In AODV, two techniques are used most frequently:

* Route discovery
* Route maintenance

Path discovery involves the source communications inan RREQ packet in the direction of the target, which replies by transmitting an RREP packet, and the destination determining the route to the source. Then, following the route of the RREQ, the RREP adds this item to its route database. Alternate Path Routing Table (ART) and Primary Routing Table (PRT) are the two routing tables that are present on each node ART. Each entry in PRT is unique for a destination node. Here, PRT is used for the indication of an entry for any target in node X's routing table.

Route Maintenance: The process of route maintenance begins once a fault on the route is discovered. When a route failure in the current path is discovered, the procedure is started.

This study also deals with the fault tolerance for provision of a fault tolerance-based AODV protocol, which addresses the issues of robustness and fault tolerance in WSN [19]. Designing of a backup route for each node on the primary line of data transmission, helps creation of the fault tolerance mechanism. The node immediately uses its backup route for conveying the incoming data packets in the place of the previous broken route devoid of interfering with transmission of data for a decrease in the amount of data packets dropped due to failure of path and to maintain the stability of data packet delivery in the occurrence of faults on the major path on transmission of data.

IoT items, like many other things in everyday life, are susceptible to failures either as a system as a whole or as an individual object. Conformation of the failure conforms to a certain probability distribution without losing generality could be assumed. Therefore, it's crucial to investigate the IoT's dependability and availability measures through investigation of the characteristics of devices as well as the devices themselves. The IoT device dependability metric is defined as the period of time during which the device is continuously operational in this concern. Thus, the chance of an IoT device being in operational condition within the range [0, t] may be used for the construction of the reliability metric R(t). The suggested system is needed for the assessment of the fault tolerance of IoT applications.

(11)

The proposed FAODV routing protocol enables the offer by the shortest path AODV offers speedy and effective route construction between nodes requesting communication between participant nodes intending to create and maintain a fault-tolerant WSN. Route selection metrics include the number of hops on a path. The shortest hop count route is selected when the source receives several RREPs with a similar destination sequence number. Additionally, There is some reduction in implementation complexity with the removal of a number of components for the ongoing AODV aspects. The Hello, RERR (Route Error), and RREP-ACK (Route Reply Acknowledgment) messages are first made apart for a decrease in the unused control packets in the network..

**Algorithm 2: AODV protocol for fault tolerance and work attack detection**

Start

500 nodes in given IoT based WSN network

Do CH node selection via EFF algorithm

Select the best CH node from the cluster member

Cluster member sends the data packets to CH node

Establish the shortest path route using route discovery and maintenance process

If valid route in routing table, then start the data transmission

Else

Start route discovery

Detect early malware

When Particular node is S and I node

Assign the particular node as malware node

Then

Discard the S and I node

When Particular node is E node

Assign the particular node as malware node

Then

Remove the malware attack from the node

Return the node as R node

When main route gets failure

Then

Apply fault tolerance mechanism via (11)

Create backup route

Transmit the number of packets through backup route

Return all possible shortest paths

Select the best short routing paths

Continue data transfer

Stop

The above Algorithm 2 describes the best shortest routing path selection using optimal parameters. The protocol has the ability to handle topology and routing information recognition to on-demand route discovery, maintenance of the route and the use of node series numbers. The malware attack detection is carried out as effectively as possible for enhancement of safe transmission of data into IoT based WSN. The FAODV uses the best CH in the choice of the optimal route and for routing through enhanced measurements. AFODV obtains routes on demand and IoT-based WSN nodes operate collaboratively and effectively by exchanging different information based on bandwidth, energy utilization, minimum distance and shortest travel routes.

Fig. 2 is the overall block diagram of the proposed system. Initially, the number of nodes is considered in IoT based WSN. Then, the system model is constructed using these nodes. Following this CH node is selected via EFF algorithm. It generates the best fitness values for energy consumption and delay metrics. The higher brightness of fireflies indicates lower energy consumption node and delay nodes elected by EFF algorithm. Finally, malware detection is done with the use of FAODV protocol. By strengthening the fault tolerance mechanism of the AODV protocol, it addresses the difficulty of robustness and fault tolerance in WSN. Therefore, investigation of the IoT's dependability and availability measures becomes a crucial issues by looking at the features of devices and devices themselves. The malware attack detection done optimally improves secured data transmission in IoT based WSN

Construct IoT-WSN system model

Performance evaluation

**CH node selection using EFF**

Compute the best fitness value

Find and select the suitable CH node

Sensor nodes in IoT based WSN

**Ensure malware attack detection, fault tolerance and routing path using FAODV**

Detect the malicious node

Ensure shortest path routing

**Fig 2 Block diagram of the Present system**

1. **Experimental result**

This part, deals with the assessment of the effectiveness of the proposed EFF-FAODV protocol and contrasted with other approaches like the SEIR-F model [14] and the Deep Learning (DL) technique [20].Table 1 depicted the simulation parameters, and the NS-2 tool is used to simulate this study End to end delay, energy utilized, throughput, packet delivery ratio and network longevity of the current and suggested approaches are compared.

**TABLE 1: SIMULATION PARAMETERS**

|  |  |
| --- | --- |
| **Parameter** | **values** |
| Nodes | 100-500 |
| Size of the Area | 1500 \* 1500(Meter) |
| Mac | 802.11 |
| Routing protocol | AODV |
| Overall energy | 150 Joule |
| Initial value of energy | 1.5 Joule |
| Radio Range | 250m |
| Simulation Time | 200 sec |
| Size of the Packet | 80 bytes |

In End-to-end delay t is a phrase use to explain the time it obtain for a packet to travel across a network as of its source to its destination. It is a phrase utilized for description of the period require at for a packet to travel across a network from its source to its destination.

(12)

Where is the ith packet's receiving time, where n is the overall packets, and is the sending time of the ith time.

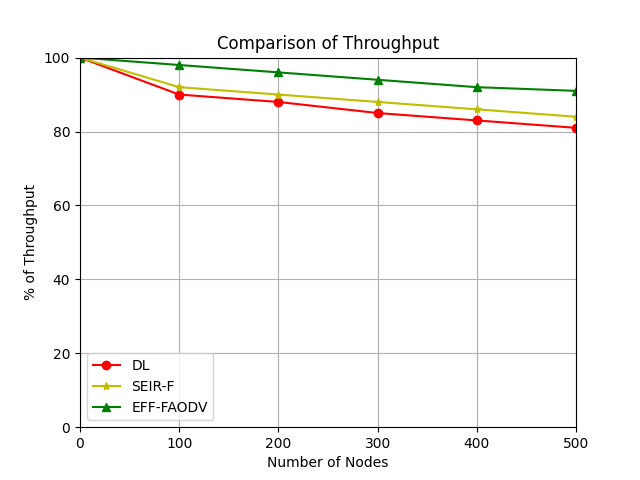
Figure_1

**Fig 3 End-to-end delay comparison**

Fig 3 shows the comparability between how the DL and the current DL, SEIR-F algorithms and proposed EFF-FAODV protocol for the end to end delay performance. The number of nodes and end-to-end latency metrics are shown on the x- and y-axes, respectively. The suggested EFF-FAODV protocol over the IoT based WSN help reduction in , the time needed to send data during the secured data transmission process. The lower energy node transfers data packets to the higher energy sensor nodes for enhancement of the data collection process. With the outcome the sink node uses the shortest pathways for getting the necessary data from the superior energy sensor nodes. The proposed EFF-FAODV protocol provides efficient path routing in IoT based WSN for finding malware attacks. According to the findings of the simulation, the newly suggested EFF-FAODV protocol produces a shorter delay from beginning to finish than the DL and SEIR-F approaches that are now in use.

In throughput of a network or communication channel is the phase at which data packets are efficiently agreed during its operation.

(13)



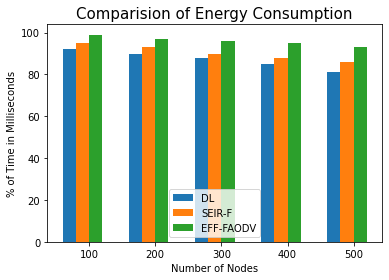
**Fig 4 Throughput comparison**

Fig 4 shows the comparability between how the DL and the current DL, SEIR-F and proposed EFF-FAODV protocol for measure for throughput. Nodes are counted on the x-axis, whereas throughput is measured on the y-axis. The proposed EFF-FAODV protocol is used for determination of the malware attacks using S, I, E criteria of R Node effectively in IoT based WSN. This helps accurate collection and transmission of the secured data without any information loss across many nodes. It demonstrates the outperformance of the suggested EFF-FAODV approach over the current DL, SEIR-F methods in conditions of throughput.

In Energy consumption **t**he average amount of energy required over time to send, receive, or forward a packet to a network node is referred to as energy consumption.

(14)

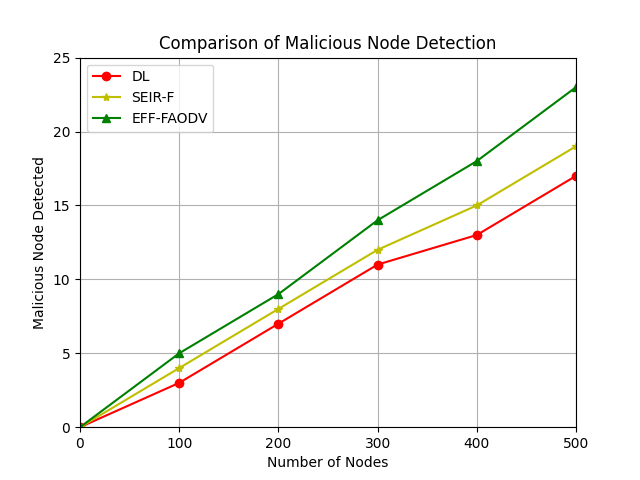
The data packet, where pi, energy required for packet transfer i, where d is the distance among the communication node and the target node, and is the energy required to receive the message.



**Fig 5 Energy consumption comparison**

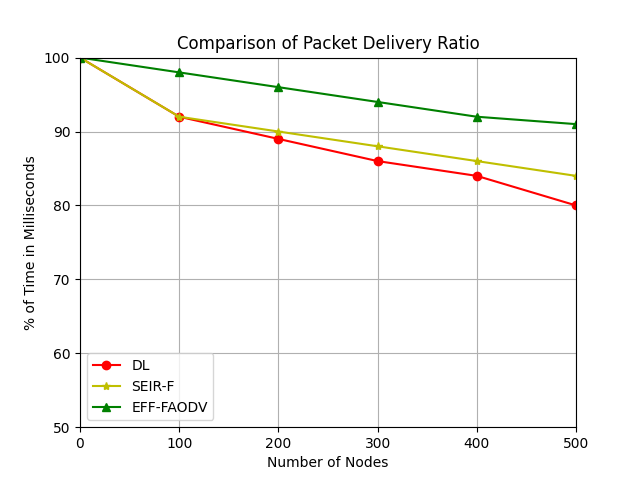
Fig. 5 shows the proposed EFF-FAODV protocol and the SEIR-F and DL protocols that are already in use are compared for the energy utilized. The y-axis procedures energy utilize, with the x-axis detailing procedures the amount of nodes. For the period of the data packet transmission, utilization of energy experiences reduction with the facility of projected EFF algorithm over the IoT based WSN.The use of CH-based data allows for the classification of sensor nodes according to the degree of residual energy. The optimal shortest route routing is built using the EFF-FAODV protocol, which is utilized for increase in energy consumption. It shows the suggested EFF-FAODV protocol utilizing a smaller amount energy than the currently used methods, which utilize extra energy.

The below figure 6 shows that malicious node detection detection rate as small compared with the existing approaches. Consider 5 malicious nodes for 100 nodes in all out of 500 nodes with the malicious nodes as 25. The EFF+ FAODV method can detect out of 25 nodes 23 nodes are indicating the efficiency of proposed method compared to other previous protocols. It is shown in the Fig. 10. Even though numerous of nodes deployed in every round are increased, the malicious activity is controlled by prevention. As a result, it illustrates how the proposed EFF+ FAODV approach is employed to achieve safe and well-organized data transmission in WSNs.



**Fig 6 Comparison of Malicious Node Detection**

**In Packet Delivery Ratio (PDR) t**he quantity of packets effectively sent to the destinations is referred to as the packet delivery ratio.



**Fig 7 Packet delivery ratio**

A comparison of the proposed EFF-FAODV protocol with the current DL, SEIR-F, and SEIR-F in expressions of packet delivery ratio may be seen in the aforementioned Fig. 7.The amount of nodes and PDR values are represented on the x and y axis, respectively. DL and SEIR-F approaches are used to reduce PDR values in the current situation.PDR value is greatly boosted in the suggested method by using the proposed EFF-FAODV protocol. Thus it shows the performance of efficient and secured data transmission in IoT based WSN using the proposed EFF-FAODV protocol.

1. **Conclusion**

In this work, EFF-FAODV approach has proposed for optimizing the CH node chosen. The shortest path routing along with malware detection over IoT based WSN. EFF techniques have been suggested for identification of the optimal CH node selection. Lowering of the hop count of nodes and applying the best fitness values, helps utilization in the selection of the most excellent CH node. By taking into account remaining energy and end-to-end latency as its fitness function, the best solution is generated in the CH node selection process. The focus of AODV protocol is on improvement of shortest path routing by utilising route discovery and route management functions in order to boost the coordination of IOT based WSNs. FAODV protocol avoids the malware attack nodes and therefore the packet loss is reduced prominently.Then, fault tolerance mechanism is applied for handling the route or node failure. The mission-critical function of the sensor network shouldn't be impacted by sensor node failure. In spite of component failures, fault tolerance refers to a capacity of a system to continue performing the required service. The performance of IoT-based WSNs is improved by FAODV, which uses fault detection and fault recovery. The findings of the study show out performance of the recommended EFF-FAODV procedure over the approaches in conditions of network lifetime, throughput, PDR, end-to-end latency, and energy consumption. To deal with computational overhead difficulties effectively, may become a subject of future study. Design of a hybrid swarm optimization and innovative encryption technique.

**Declarations:**

**Funding:**

* The authors did not receive support from any organization for the submitted work.

**Competing Interests:**

* The authors have no relevant financial or non-financial interests to disclose.

**Data Availability:**

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

**Author Contribution:**

All authors have contributed equally.

**References**

1. Harihara Gopalan, Vignesh V, Udaya Suriya Rajkumar D, Velmurugan A K and Deepa R Dhanapal (2024). Fuzzified swarm intelligence framework using FPSOR algorithm for high-speed MANET-Internet of Things (IOT). Measurement: Sensors,31(2), 1-8 .
2. Wu, Wenliang, Naixue Xiong, and Chunxue Wu.(2017).Improved clustering algorithm based on energy consumption in wireless sensor networks. IET Networks, 6(3),47-53.
3. Thakkar, Ankit, and Ketan Kotecha. (2014).Cluster head election for energy and delay constraint applications of wireless sensor network. IEEE sensors Journal, 14(8), 2658-2664.
4. Vullers R J M, Schaijk R V, Visser H J, et al.(2010). Energy harvesting for autonomous wireless sensor networks. IEEE Solid-State Circuits Magazine, 2 (2),29-38.
5. Wu, D., He, J., Wang, H., Wang, C., & Wang, R.(2015).A hierarchical packet forwarding mechanism for energy harvesting wireless sensor networks. IEEE Communications Magazine, 53(8), 92-98.
6. Shen, S., Huang, L., Liu, J., Champion, A. C., Yu, S., & Cao, Q (2016). Reliability evaluation for clustered WSNs under malware propagation. Sensors,16(6), 1-20.
7. Mosavvar, Islam, and Ali Ghaffari (2019).Data aggregation in wireless sensor networks using firefly algorithm. Wireless Personal Communications,104(1), 307-324.
8. Acarali, Dilara, et al. (2019).Modelling the spread of botnet malware in IoT-based wireless sensor networks. Security and Communication Networks, 10 (115), 1-13.
9. Omar A. Alzubi, Jafar A. Alzubi, Moutaz Alazab, Adnan Alrabea, Albara Awajan and Issa Qiqieh (2022). Optimized Machine Learning-Based Intrusion Detection System for Fog and Edge Computing Environment. Electronics, 11(19),1-16.
10. Vijayalakshmi, K and P. Anandan. (2019). A multi objective Tabu particle swarm optimization for effective cluster head selection in WSN. Cluster computing, 22(5), 12275-12282.
11. Rose, SG Hymlin, and T. Jayasree. (2019). Detection of jamming attack using timestamp for WSN. Ad Hoc Networks, 91(3), 1-12.
12. Ojha, Rudra Pratap, et al. (2021). Improved model for the stability analysis of wireless sensor network against malware attacks. Wireless Personal Communications,116(3), 2525-2548.
13. Mohapatra, Hitesh, and Amiya Kumar Rath. (2020). Fault‐tolerant mechanism for wireless sensor network. IET wireless sensor systems, 10(1), 23-30.
14. Xu, Biao, Minyan Lu, Hong Zhang and Cong pan. (2021). A novel multi-agent model for robustness with component failure and malware propagation in wireless sensor networks. Sensors, 21(14), 1-25.
15. Udaya Suriya Rajkumar D, Shanmugaraja P, Arunkumar K, Sathiyaraj R and Manivannan P (2023). A HSEERP- Hierarchical Secured Energy Efficient routing protocol for wireless sensor networks. Peer-to-Peer Networking and Applications, 17(1), 163-175.
16. Liu, Jingsen, et al (2020). A dynamic adaptive firefly algorithm with globally orientation. Mathematics and Computers in Simulation, 174, 76-101.
17. Sai, Van-Oanh, et al. 2015. Parallel firefly algorithm for localization algorithm in wireless sensor network. 2015 Third International Conference on Robot, Vision and Signal Processing (RVSP). 300-305.
18. Zhang, De-gan, et al. (2015). Extended AODV routing method based on distributed minimum transmission (DMT) for WSN. AEU-International Journal of Electronics and Communications, 69(1), 371-381.
19. Mohapatra, Hitesh, and Amiya Kumar Rath.(2020). Fault-tolerant mechanism for wireless sensor network. IET Wireless Sensor System, 10(1), 23-30.
20. Ateeq, Muhammad, et al.(2019). Multi-parametric analysis of reliability and energy consumption in IoT: A deep learning approach. Sensors, 19(2), 1-20.
21. Rajkumar, D. U. S., et  al. (2019). Artifcial bee colony method for identifying eaves dropper in terrestrial cellular networks. Transaction Emerging on Telecommunication Technology, 10(1002), 1–17.
22. Udaya Suriya Rajkumar, Raj Anand and Sathiyaraj (2021).A Centralized Mechanism for Preventing DDOS Attack in Wireless Sensor Network. Wireless Personal Communication, 10(1007), 1191-1208.
23. Nima Jafarzadeh, Ahmad Jalili, Jafar A. Alzubi, Khosro Rezaee, Yang Liu, Mehdi Gheisari, Bahram Sadeghi Bigham, AmirJavadpour.(2022). A novel buffering fault‐tolerance approach for network on chip (NoC). IET Circuits, Devices & Systems, 10(1049), 250-257.
24. Omar A. Alzubi, Jafar A. Alzubi, Ala' M. Al-Zoubi, Mohammad A. Hassonah, Utku Kose, (2021). An efficient malware detection approach with feature weighting based on Harris Hawks optimization. Cluster Computing Journal,10(1007), 2369-2387.
25. Omar A. Alzubi, Issa Qiqieh, Jafar A. Alzubi. (2023).Fusion of deep learning based cyberattack detection and classification model for intelligent systems.Cluster Computing Journal, 26(2), 1363-1374.