Trust-Enabled Energy Effective Optimal Framework for Detection of Intrusions in the Network Using AI Scheme

Putty Srividya (srividyaosmania@gmail.com)
Osmania University
Lavadya Nirmala Devi
Osmania University

Research Article

Keywords: WSN, Trusted node, probabilistic Cuckoo search Node optimization algorithm, weighted-Biased end-to-end delay approach.

Posted Date: September 17th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-906210/v1

Trust-Enabled Energy Effective Optimal Framework for Detection of Intrusions in the Network Using Ai Scheme

Putty Srividya[1]and Dr. Lavadya Nirmala Devi[2]
[1]Assistant Professor, [2]Professor
[1,2]Dept. ECE, University College of Engg.
[1,2]Osmania University, Hyderabad, India.

Email: [1]srividyaosmania@gmail.com, [2]nirmaladevi@osmaina.ac.in

Abstract. Wireless Sensor Networks (WSN) are self-possessed of the devices that are capable of actuating/sensing, processing, and communicating. This is employed for enhancing the day-to-day life, moreover secure data transmission was regarded as the major challenging aspect for the deployment of data. Data dissemination is a crucial in the complex communications framework for transferring messages for any given condition on the network. The dilemma of fixing the safest efficient route was a tedious issue. Hence the secure and most reliable way will give the appropriate solution for the routing issues. Here in this paper the Trust based energy efficient route path identification by Multi-faceted biologically-inspired probabilistic Cuckoo search Node optimization algorithm (TEERP-MFBPCS)is employed to find the efficient safest route within a short period. After seeing the efficient route, the node can be distinguished upon the traffic and security. Then in the selected route, the nodal distance can be calculated through applying weighted-biased end-to-end delay-based approach for traffic analysis. Finally, the intrusion node can be detected and the performance analysis is carried.

***Index Terms*—**WSN, Trusted node, probabilistic Cuckoo search Node optimization algorithm, weighted-Biased end-to-end delay approach.

1. Introduction

A distributed and self-organized WSN is a series of autonomous small-scale sensor nodes working together towards a common target. WSN has small sensor nodes composed of sensor modules, data processing and connectivity. WSN is a series of several sensor nodes densely distributed for military and civil applications in harsh environments. WSN typically consists of a base station capable of communicating through a radio communication with a variety of wireless sensors[1, 2]. Wireless sensor node data is processed, compressed and sent directly to the base station. WSN has many restrictions such as a low processing power, poor memory, insufficient energy resources[3, 4], the use of unsecure wireless networks and the use of sensor nodes in an unattended environment. Selective transport attacks, Wormholes attacks, Sinkhole attacks, Sybil attacks, HELLO flood attacks, Acknowledgment spoofing, sniffing attacks, energy dump, black hole attacks, service attacks deviation, smugglers research attack, privacy breach attacks and clone attacks are different possibilities of attack on the WSN. An enemy can catch and extract the core materials from a sensor node. The intruder will reprogram the node to create a replica of the node captured after a node has been captured. These copies should be found in all network zones (or replicas). These node replica attacks are very risky for sensor network operations. The intruder will create as many replica nodes as he needs from a single captured sensor node. The adversary forbids the replica nodes, but it does have key materials which make them appear to be approved network members. A clone attack is also very difficult to detect [5, 6]**.** WSN can be mobile or static. Randomly, nodes are used in static WSN sensors and do not change their locations after deployment. In mobile WSN, after installation, the sensor nodes will shift themselves. There are centralized and distributed two forms of detection technologies in static WSN.

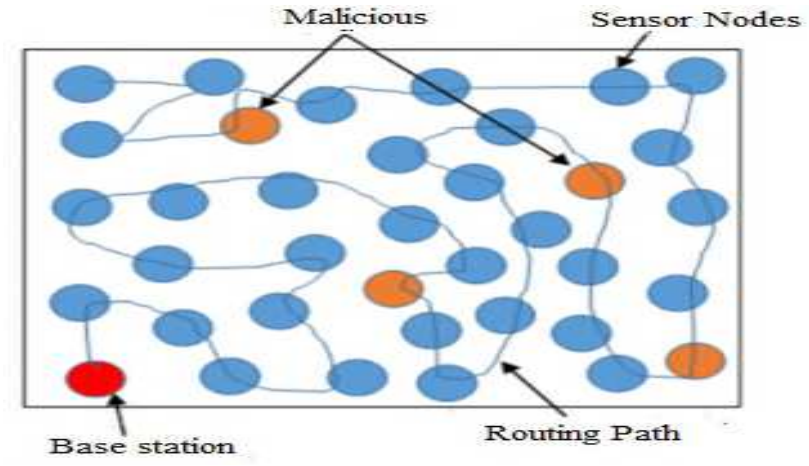

Figure 1 Malicious node identification in WSN

When a new node joins the network, it broadcasts a location demanded containing its location and name to its neighbors in a core method for node replication. This argument was then forwarded to the base station by one or more of his neighbors. The base station can quickly detect any pair of nodes with the same identity but at many locations with location information for all nodes in the network. Making compromise with the base station or obstruct the route to the base station, opponents can incorporate any number of replicas in the network, is the key drawback. The node deployment in WSN is shown below:

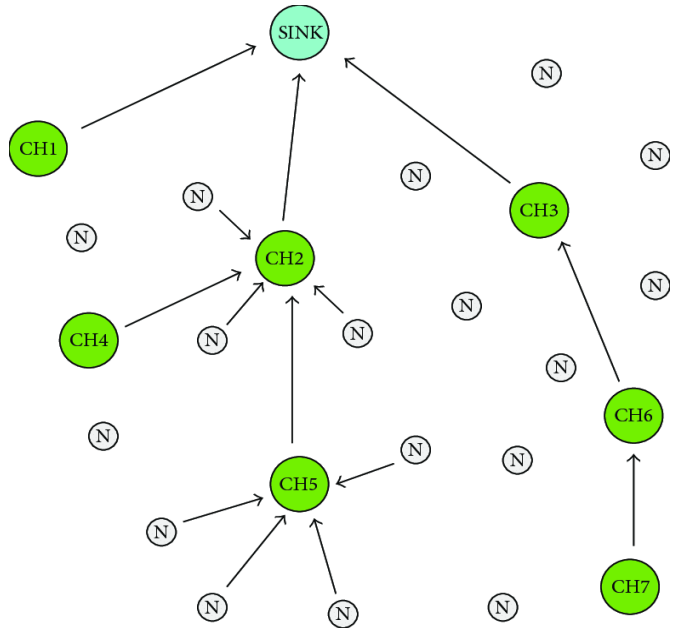

Figure 2 Node deployment in WSN

When a new node connects to the network, its retention to the related witness nodes is redirected. If there are two location statements obtained by a witness node for the same node ID, the presence of the clone is acknowledged. There are several methodologies are presented in the existing work for the detection of clone attack but each of them possesses some disadvantage. Hence here in this paper to overcome the malicious node identification associated issues, a novel scheme was implemented here in this paper.

The main intentions of this work are as follows:

- To propose the trust-based energy efficient optimization scheme to find trusted node with efficient

path.

- To introduce Trust based energy efficient rout path identification by Multi-faceted biologically-inspired probabilistic Cuckoo search Node optimization algorithm (TEERP-MFBPCS)for providing trusted path with energy harvesting and to identify authentic nodes.

- To introduce weighted based end-to-end delay framework for data transmission.

The residual portion of the paper is systematized as shown: section II is the deliberation of various existing mechanism employed so far. The detailed explanation of proposed system is offered in section III. The estimation of performance is illustrated in detail in section IV. At last, the conclusion summarizes the overall workflow of proposed strategy.

2. Related Works

[7]formulate Proposed design of a Cuckoo search algorithm (ARP-CS) adaptive routing protocol. The adaptive protocol integrates the functionality of both topology and geographical protocols, which guarantee a safe data transmission with less time and a high delivery ratio for packets.

[8]proposed the congestion control framework for adaptive beacon generation (ABGR) was suggested to ease congestion and containment of the channel. The beacon generation frequency can be progressively modified as per different volume rates so that the beacons are transmitted accurately and timely. Dynamic application-level quality testing scheme (T-Pro) was proposed to determine the performance of multiple security systems at different densities. It is focused on a comparison between traffic density and speed. Ultimately, three security implementations were tested using the method ABGR for their applicability consistency.

[9]proposed a fog computation (FC), including the CUC, the firefly algorithm (FA), the fire-fly NN (neural network) and a KDE (key-distribution) facility intended for validating the node level and network level together in contradiction of any reliability attack, in the hybrid optimization algorithms context (OAs).

[10] Implements a protected analytical routing modeling that tracks the malice of the surrounding node reliably and allows choices for stable routing through the source nodes. The suggested framework is able to leverage the ability for conceptual probabilistic modeling and can also be used to resist maximal number / threats in the wireless network. [11] The Exponential Reliability Credibility Mechanism (ERCRM) has been developed, in which the autonomous nodes are isolated using an exponential reliability coefficient, from the routing route. A value dependent on the matrix for increasing network protection and stability is expected in the scheme.

[12] considered the optimization algorithm of ACO that decreases the consumption of energy. [13] presented a technique of hash-proof for securing user's data by preventing them from leakage attacks[14].[15]In order to detect misbehavior or irregulars and node acts, IDSs are distributed as numerous agents across the network. Agent information is obtained by sensors. The extracted information is then processed for further processing. The attacks can be stopped by reporting information from malicious nodes to the linked IoT objects or to the administrator.

[16] proposed a new safe routing algorithm is proposed, called an energy-conscious confidence-safe routing algorithm, where an estimation of confidence score is used in order to efficiently identify the malicious users in WSN. Experiments have shown that, as compared with current security, energy consumption and packet delivery systems, the proposed trust-based routing algorithm achieves substantial enhancements to its performance.

[5] here in which wireless network interdiction/protection issue where a protector positions a series of hub locations to deploy jamming equipment to reduce the costs involved with the construction of hubs and the use of electricity before and during jamming attacks. The goal of the intruder is to identify the places where jamming devices can be deployed and to interrupt the wireless network operation to increase consumption of energy. It is a quadratic bi-level problem that we formulate this. A search algorithm on 48 randomly generated networks is

applied and test.

[17] proposed a new and effective clustering of SN through the use of Spectral Graph Theory, called Eigen Values (CEV), is suggested in this paper. This article uses the Laplacian matrix for spectral clustering theory. For the grouping of the WSN nodes are used the autonomous values of the Laplacian matrix and its related function. Using smooth reasoning and energy and distance limits, CH is chosen. Evaluation of results in this study is analyzed and contrasted to LEACH and HEED.[18]Examine energy-intensive algorithms and network life on WSN to enable a variety of applications. Clustering is one of the hierarchic protocols for routing between SN and sinks employing a Head Cluster (CH); various algorithms are available to select the appropriate CH effectively and localize cluster memberships with fuzzy logic classification parameters to limit regular clusters consuming more energy, and we have applied the neural network learn.[19] presents an energy model for the scenario and proposes a traffic and energy-aware routing (TEAR) scheme to improve the stability period.

[20] Present a new protocol for the use of Naïve Bayes intrusion detection systems algorithms (IDSs). Moreover, because of their decreased installation and operating costs, the IDS-based systems are more workable for the IoT environment. [21] Proposes a function-based, trustworthy neighbor activation to improve network security in resource-constrained WSNs. AF-TNS operates in two phases: energy constraint confidence assessment and metric node assessment to maintain community confidence. The random transigmoid feature simplifies the dynamic decision-making mechanism of the AF with a differentiation between trustworthy and unconfident network results. Simulation findings indicate that AF-TNS increases network efficiency by improving the identification rate and maintaining the lifespan of the network.

[22] Propose the new Energy Efficient Routing Protocol (QoS), a confidence and energy modeling protocol developed in order to enhance the protection of the WSN and also to optimize energy use, known as the Stable Standard of Services (SQO). [23] the Detailed Trust Management Method (GDTMS) for F-IWSN is proposed by Gaussian distributor. In addition, the grey decision is adopted in its trust decision to put in a trade-off between protection, transmission efficiency and energy consumption. The proposed deal will effectively pick the safe and stable transmission node, namely a secure routing mechanism based on trust management.

[24] implements Advanced Encryption Standard-enabled protocol for Secure Routing Trust that depends on suggested energy and confidence protocol of the Dolphin Cat Optimizer (AES-TDCO). In addition to length of time, distance and related time, the proposed Dolphin Cat Optimizer is used to ensure best path assortment based upon the demonstrated objective role of confidence variables and historical trust, current trust, indirect and direct trust.

[25]Proposed a scheme using Aumann Agreement Theorem based on Truth Convergence for attack detection and prevention. The comportment of nodes is extracted and their patterns are established. In the basis, it anticipates potential network attacks.

[26] Proposed an Ad hoc Trust Alert protocol that measures the degree of trust between the nodes and transmits data safely between nodes. It predicts a confidence value dependent on calculating distance by electricity, mobility and RSSI. This protocol offers neighbor information to report the success and failure rate of the transfer of packets.

3. Proposed Work

The narration of proposed system workflow is provided in this section. The main intentions of this work are as follows: To propose the trust-based energy efficient optimization scheme to find trusted node with efficient path. Trust based energy efficient rout path identification by Multi-faceted biologically-inspired probabilistic Cuckoo search Node optimization algorithm (TEERP-MFBPCS) are presented for providing trusted path with energy harvesting and to identify authentic nodes. To introduce weighted based end-to-end delay framework for data transmission.

The proposed system overall workflow is shown below:

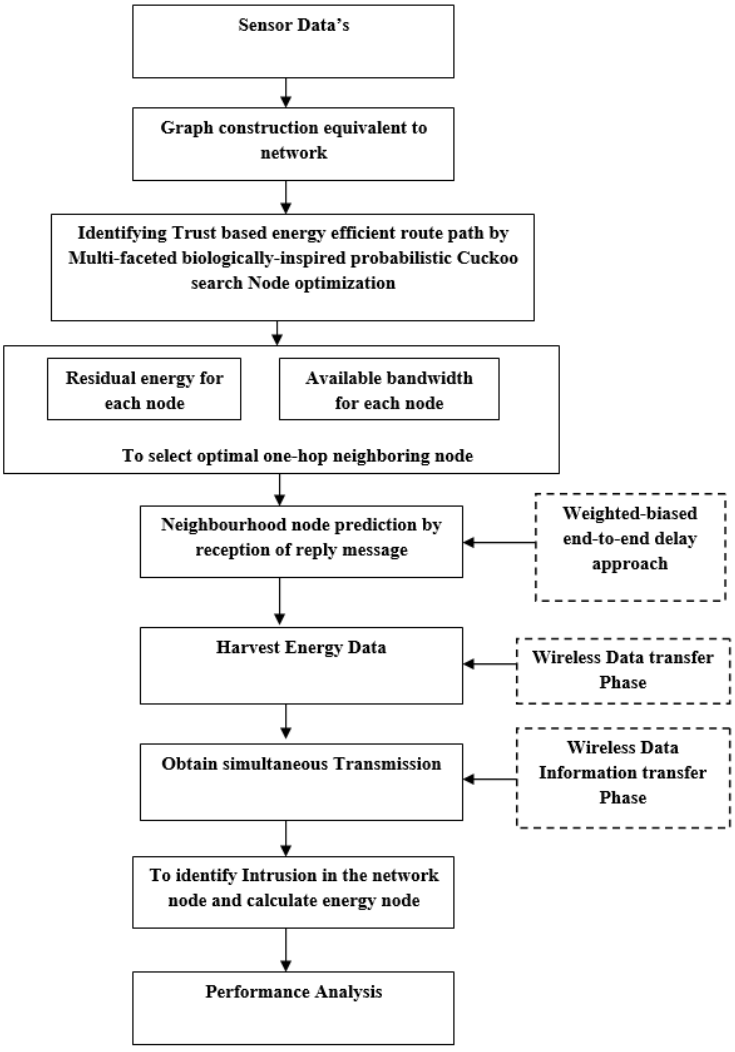

Figure 3 flow of proposed system

A. System Model

Initially, two general models were presented to suggest the transformation of information among nodes in the system. It was assumed that there was an N number of nodes that were moving at some distance as per the reference region model of group mobility. The entire nodes in the model have an equivalent range of transmission. Each node is capable of transferring information to the neighboring nodes. The coordinates are regarded as the location information sent by nodes at two consecutive time's t1 and t2, correspondingly. To examine simplicity, it was presupposed that one node is fixed, and another node is moving, however, actually, they are all moving at the entire time period. At this time, it is understood that nodes maintain their direction and velocity at the duration $\Delta t = t2 - t1$ and reach the destination at the moment t2.

B. Identification of energy efficient route path:

For the identification of energy efficient routing path, a heuristic cuckoo search optimization technique is employed. To each nodethe control messagesare transmitted as an alternative which in turn will broadcast it to specific nodes that are selected and are known as multipoint relays. The task of multipoint relay was the dissemination of messages in the network.

The routing protocol has been adapted through several energy efficiency techniques. At this, one enhanced Method has been presented for storing several shortest paths in the routing table that in turn will reduce re-run routing algorithm redundancy for recognizing the shortest path from topology table and also will use a smaller amount of energy. In this article, residual energy will count up nodes and the Packet will be forwarded to those nodes who comprise high enduring energy in addition to simply that nodes will send the entire nodes packet in the system. The proposed work will adapt routing protocol for the reason of less energy consumption n by varying the hello message by means of residual energy field addition. Before sending hello message, every node adds its own enduring energy in hello message and include residual energy field inside the TC message.

The energy efficient routing identification depends on following: node connection, delay, quality, link-state, and QoS metrics in the network.

(i) Node Connectivity: Each node should identify the neighbor nodes. It has a direct and directional link in the network. For this, every node transmits its messages periodically, having the neighbors list known to the node and its link position. The messages that are obtained by all one-hop neighbors are not promoted. Depends on this message, every node knows the total neighbor nodes that are linked to it directly.

(ii) Delay: It is the time seized among the two nodes for which a source node n1 throws a message to destination node n2 and delivers successfully. Every node contains in the message the formation time of this corresponding message. When a neighbor node be given this message, it computes the divergence among sent time and the present time in a harmonized network.

$$\text{Delay} = \sum_{0}^{N}\left(\frac{\text{obtainedtime} - \text{senttime}}{N}\right) \quad (1)$$

(iii) Quality: It describes the link capacity among the two nodes n1 and n2. The link quality is calculated on the exchanges of the information periodically from each other.

$$\text{Quality} = \frac{\text{HM1hopU}}{\text{TMHhopV}'} \quad (2)$$

HM1hopU, Hello message N received from 1 hop; THM1hopv, Overall message 1-hop has sent.

(iv) Link State: Link state shows the status of the link at a given time T.

(v) QoS metrics: The available link bandwidth among two nodes n1 and n2 is equivalent to the highest of their idle time increased by the most significant bandwidth. Consequently, it depends on the given values, QoS metric satisfaction is calculated as in:

QoS metric Satisfaction = (Q+BW) – CD (3)

Where Q is quality, BW is Bandwidth, and CD is Computational Delay.

A set of services necessities are congregated by network, while transferring data packets from source to destination node. QoS metric satisfaction describes in terms of one or set of parameters in the system such as delay while data transmission, Bandwidth, Jitter-delay, Packet loss etc. It is imagined that the packet-level Quality of Service (QoS) is guaranteed by assigning as a minimum bandwidth. The goal of QoS satisfaction is to build stable clusters by thinking about the mobility of the sensor node. In network, stable cluster formation is incredibly necessary for superior QoS as the metric performance satisfaction. To gratify the QoS guarantees traffic instruction cooperate a central task in the network. i.e., it becomes required to sustain per-flow or per-class situation information via control of Admission and traffic policing method.

C. Dijkstra's path routing to reduce energy utilization

The Dijkstra process was employed in routing frequently and the other protocols related to network. This proposed algorithm in turn estimates the shortest path from a given source node to all of the other sensor nodes. It needs the all-edge's weights were not negative. It functions through sustaining a visited sensor nodes set and revising continually the uncertain distance to all of the unvisited sensor nodes. At every iteration, the nearby unvisited sensor node is adjoined to the visited sensor node-set, and the distances among its unvisited neighbor's nodes are updated. Dijkstra's algorithm employs with non-negative edges. Nonetheless here, the signal strengths that were robot take negative or zero principles. Consistent with these signal strength values, if the signal strength is among the exposure area. Uncertainty the strength of signal is just below -93, after that the automaton is beyond areaof coverage. Now, a reliable destination gets established based on Dijkstra's algorithm. So as to employ this Dijkstra's algorithm in the research work request, in this the robot signal strengths normalized as,

$$\text{Cost (a, b)} = \begin{cases} -93 \le \text{Sa, b} \le 0 & 1 - (\text{Sa, b}/100) \\ \text{Sa, b} < -93 & \propto \end{cases}. \quad (4)$$

In the stated mathematical equation Sa, b is employed for representing the strength of signal value among the robot ith and jth robot. Cost (a, b) was employed for describing the value of link cost amongrobot ith and jth robot that was employed by this algorithm.

By concerning the Dijkstra's algorithm, the optimal and reliable data transmission gets found. Now, the data gets transmitted reliably and secured manner. Here, the performance analysis brings establish in the following section.

C. Trust based energy efficient rout path identification using Multi-faceted biologically-inspired probabilistic Cuckoo search Node optimization algorithm (TEERP-MFBPCS)

The best way of selecting a route is usually for prediction of traffic among the source and the destination end in sensor routing. The density of low traffic direction of a low traffic density is favored for optimum route choice, as a high traffic density increases the flow of sensor nodes. For choosing the best path, therefore, an active prediction method is necessary. Route exploration is the central process in the current implemented method. The optimization algorithm finds the right route, from source to destination, which meets the entire considered multiple limitations. For optimizing multipath, an algorithm can be used to provide reliable data delivery. During the route selection, the data transfer to the destination can be postponed if the nodes are not efficient of energy and loaded because of high traffic. Therefore TEERP-MFBPCS algorithm is recommended for routing optimization. The proposed algorithm chooses the optimal multipath routing to provide the information efficiently. In case of efficient route recognition there is a need to initialize the parameters. For initializing the

upper and lower band parameters, the mutation probability and nest size is being computed. The selection of proper nest is a necessary one.

$\beta = \beta_{max}$-($N_{iter}/N_{iter(total)}$*$\beta_{max} - \beta_{min}$ (5)

Where β_{max} and β_{min}signifies the minimum and maximum size of nest, N_{iter}indicates the present number of iteration$and N_{iter(total)}$signifies the iteration number correspondingly. As per the narration of equation, the size of nest decreases with iteration number increase. In accordance with proposed TEERP-MFBPCS algorithm, the probability of mutation is associated with the fitness function,

$$P_f(\mathrm{i})=\begin{cases} P_{f_{min}} + \left(P_{f_{max}} - P_{f_{min}}\right) * K, K < 1 \\ P_{f_{max}}/N_{iter}, \end{cases}_{\mathrm{i=1...n}} \quad (6)$$

where f= fitness(i) − f_{min}, is based on the quality of current ith solution fitness (i); and fmin signifies the present value of fitness in ith solution and the current population of global fitness function correspondingly; $P_{f_{min}}$and $P_{f_{max}}$signify the minimum and maximum probability of mutation Pa, correspondingly. As of the equation 6 it is evident that the solution of fitness will be adjusted and is proportional to K. the probability of mutation usually varies relating to the iteration number. Once the parameter gets initialized, the position of nets will be analyzed.

σ_v=($\boldsymbol{\gamma}$(1+β_p))*sin($\boldsymbol{\pi}$*β_p/2)/($\boldsymbol{\gamma}$(1+β_p 2)*${\beta_p}^{\beta_p - 1/2}$)*$(\beta_p - 1/2)^{1/(\beta_p - 1/2)}$ (7)

Where, $\sigma_v$signifies the nest's random size.

The equation (7) is written as follows:

n_p=rand(τ_{san},1)*$(u_b - l_b)$+l_b (8)

Where $n_p$signifies the position of random nest

The, the objective function should be computed for finding the nearest path of the node. The node localization objective is to evaluate the unknown nodes co-ordinates depending on the sensor nodes anchor. Each unidentified node that are separable and their anchor nodes will be estimated:

σ^2= γ^2*e_{ij^2} (9)

Where $\sigma^2$is the error variance and $e_{ij^1} is$ the unknown node′s original distance. From the equation (9) it is shown that the standard deviation was proportional to the error variance. The distance measured among the anchor node and the unidentified node distance was signified by means of following equation (10)

$e_{ij'}$=e_{ij}+N_{ij} (10)

Where $N_{ij}$is the representation of error o in the unknown sensor nodes. After that, the objective function must be computed which is regarded as the integrated mean error of anchor node and the unidentified node.

$f(x_i y_i)$=$\frac{1}{n}\sum_{j=1}^{n}(e_{ij} - e_{ij'})$^2 (11)

When the objective function gets minimized means the unknown short distance path node was easily estimated.

obj_{fn}=-20*exp(-2*$\sqrt{\sum \sigma_v}$)/2-exp($\sum \cos(2\pi * \sigma_v)/d_b$)+20exp(1) (12)

After that the alpha, beta and the gamma positions gets updated. After updating it the route can be found. Then the route response is sent from the destination, multiple paths will be transmitted to the source. The remaining energy, hop count and load of each sensor node are attached with the reply packet. The node of origin to the reply packet. The origin node then analyses the response packets obtained from several routes and determines the

quality of fitness for each route on the path. It chooses the n amount of path that has the highest fitness level and places the n paths in the descending order consistent with each path's fitness values of in the routing table of the source node and then transmits data via the fitness path. Whether the path fails, it is transmitted by the subsequent value of best fitness path. Then, if all n paths struggle to transmit information, then it begins to discover and repeat the process according to the algorithm. If RRPLY sends to the neighbor node via destination node until it reaches the sender node, the routing table is modified through attaching all of the above-listed metrics according to the reverse path set by means of dragging them up until the recipient sensor node is hit. The fitness value at sender sensor node is now determined using the formula mentioned in the algorithm 1 then it can be stored in the routing table in the form of the descending order. Now the sender sensor node actually begins transmitting data consistent with the path that having highest fitness value in the routing table of the sender sensor node, if the path fails the sender sends it with the second best fitness path, and so on. Where, F is the value of fitness for any path received and classified by the source node. Here the residual energy between each of the node and the bandwidth distance between each of the pair node can be calculated. The energy, delay metric and direct route is used to determine fitness. Here is the solution of the suggested methodology. Here the cuckoo represents the source sensor node, cuckoo's egg is the data packet send by the source sensor node. At this time the packets of data from the sensor source node are sent via the multi objective path can be delivered to the destination node. The data is passed through the unreliable power or high traffic path is dropped out.

Algorithm 1 (TEERP-MFBPCS)

Input: Network Node S_n,Node_coordinate S_c,bound limit $S_{x,}S_y$, energy parameter $S_{e,}$
Output: Optimized valued φ_p andγ_i (best route path andnest)
Step1: initialize the parameter values,
[$S_{x,}S_y$]=[Upper limit, lower limit]
Maximum_number of iteration max_{iter}=100;
Lower band l_b=S_x (1)*(S_c, 2);
Upper band u_b=max(S_c, 2)
greatestneighboringn_bProportionsd_b=size(u_b, 2)
Step 2: the nest position $n_p$initialization
N=size (n_p)
beta_pos β_p=3/2;
σ_v=($\boldsymbol{\gamma}$(1+β_p))*sin($\boldsymbol{\pi}$*β_p/2)/($\boldsymbol{\gamma}$(1+β_p/2)*$\beta_p{}^{\beta_p-1/2}$)*$(\beta_p - 1/2)^{1/(\beta_p-1/2)}$
for j=1:n
s=n_p(j,:)
u=randn(size(s)*σ_v)
v=rand(size(s))
Compute the position of nest,
n_p=rand(τ_{san},1)*$(u_b - l_b)$+l_b
step 3: calculate objective function,
to compute best near nest position,
for jj=1:size(n_p)
for i=1:size(pos_{data}, 1)+)*$\beta_p{}^{\beta_p-1/2}$)*$(\beta_p - 1/2)^{1/(\beta_p-1/2)}$
flag4ub=pos_{data}(I,:)>u_b
flag4lb=pos_{data}(I,:)<l_b
pos_{data}(I,:)=pos_{data}(i, :)*(
d_b=size(PI,2)
obj_{fn}=-20*exp(-2*$\sqrt{\sum \sigma_v}$)/2-exp($\sum \cos(2\pi * \sigma_v)/d_b$)+20exp(1)
Step 4: alpha, beta and delta positions are updated,
If obj_{fn}<α_p

$$\alpha_p = obj_{fn}$$

α_p=pos_{data}(I,:)
End
If obj_{fn}<α_p&&obj_{fn}<β_p
β_p=obj_{fn}

End
If $obj_{fn}<\alpha_p \&\& obj_{fn} > \beta_p \&\& obj_{fn}<\gamma_p$
$\gamma_p = obj_{fn}$
End
end
end

E. Weighed-biased end-to-end delay approach for neighbor node prediction

The approach of weighed end-to end delay is employed for the trusted neighbor node identification. Typically, the delay was being affected through the number of hops at which the packets of data should pass through. The length of hop among the destination and source varies as per the time.

The length of the path that is proportional to the end-to-end packet delay directly. The endwise packet delay also gets increases once the path length increases. The packet delay and path length the can be done if there will be a severe bonding between them. In the presented weighed-biased end-to-end delay method, the length of the weightage path among each nodes from the source should be computed together with shorter route computation. The trusted neighbor node is the node with limited short distance which is an authentic node. The packets can directly send to the destination node after the node information. The energy is also saved in the time saving process. That particular node broadcasts the message on a regular basis in the network. Upon receiving messages, each node updates their local tables. The focus node changes its nearby maintained Neighbor Table regularly consistent with the established messages from their neighbors. The relation lifetime and the approximate bandwidth of the neighboring nodes were determined using related information. After finding the shortest less traffic path the data could directly send from the source sensor node to the destination nodes in the network.

$$Trust_{(neighbor)} = Energy_{(node)} + Trust\ Value_{(neighbor)} \quad (13)$$

Where,

$$Energy_{(node)} = \frac{\sum(PR+PF)}{Node_{i\ to\ n}} \quad (14)$$

Here, PR and PF represents the packet received and packet forwarded respectively.

The weighed node is the node with limited short distance, lack of the link break and less traffic which is a authentic node. After that the information regarding packets node could be sent directly to the node of destination. This is somehow the process of time-saving and the energy saving one also. That particular node broadcasts the message on a regular basis in the network. Upon receiving messages, each node updates their local tables. The focus node changes its locally maintained Neighbor Table regularly according to the messages received from its neighbors. The relation lifetime and the approximate bandwidth of the neighboring nodes were determined using related information. After finding the shortest less traffic path the information can send directly from the source to node of destination.

4. Performance Analysis

In this section the proposed methodology performance TEERP- MFBPCS was analyzed precisely. Figure 4 shows the implemented system model. Here for starting up the process the node pair can be predicted as shown in figure 5.

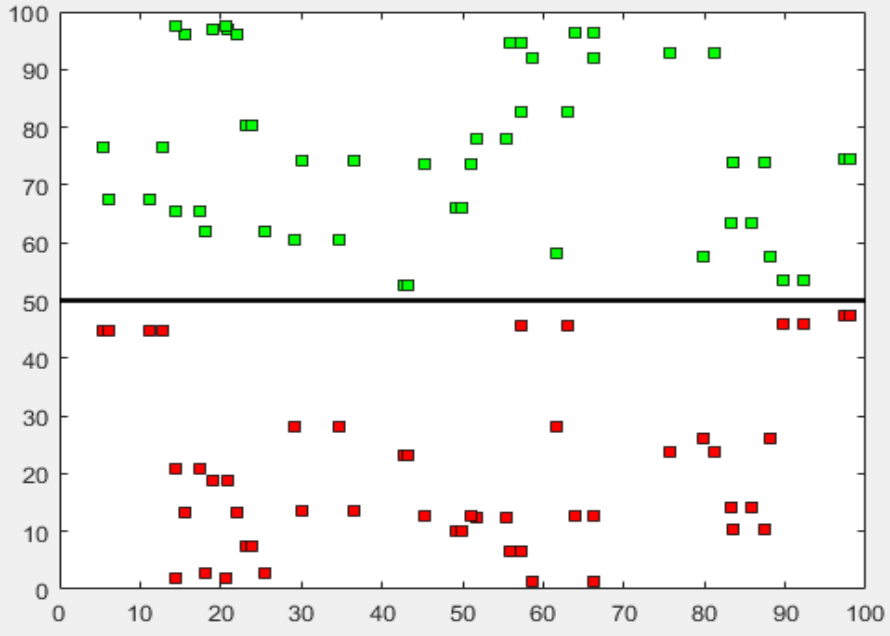

Figure 4 Implemented system model

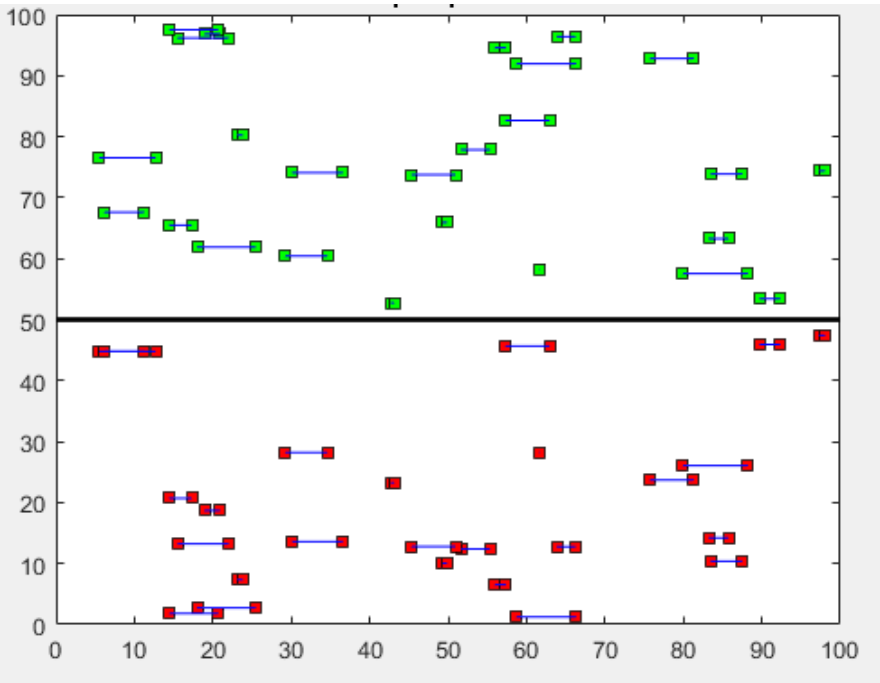

Figure 5 Node pair prediction

Then after the prediction of the node the neighbor route can be established by three methods. By using the MFBPCS efficient routing was done as shown in the figure 6. Here the residual energy between each of the nodes and the bandwidth distance between each of the pair node can be calculated.

The existing and proposed approach analysis is evaluated for both detection and packet delivery ratio. The part of data packets are delivered to the destination nodes by source node.

Table 1 analysis of maximum speed vs. PDR

Maximum speed (M/S)	TSR	ETSR-PD	Proposed
5	68	77.5	93
10	67	74.5	89
15	67	71	88
20	65.5	70	87
25	64	69	86
30	60	65.5	85

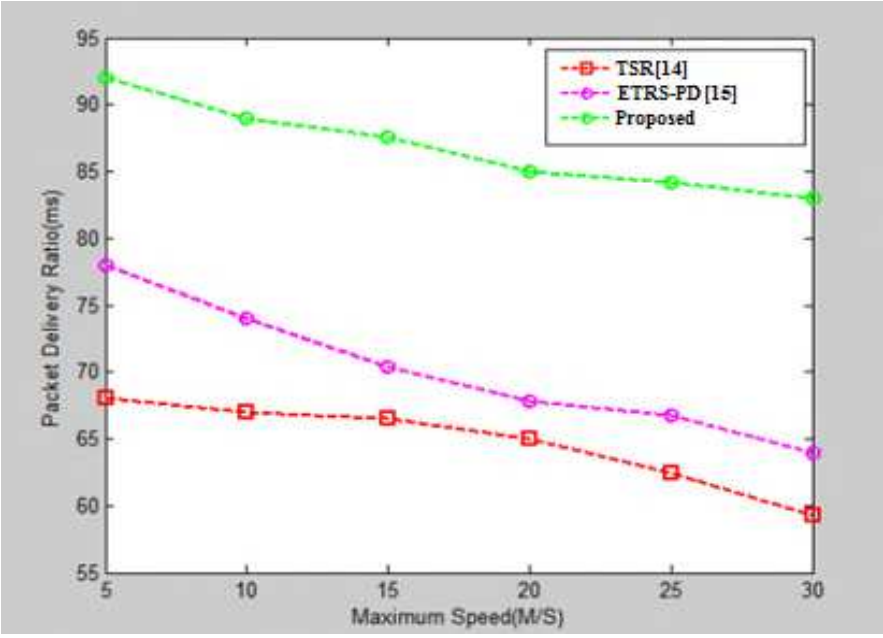

Figure 6analysis of maximum speed vs. PDR

Figure 6 reveals that TSR and ETRS-PD distribution ratios are dropping considerably with nodes that accelerate steadily relative to the suggested methodology delivery ratio. At faster speeds the variations become clearer. The approach suggested has higher distribution ratios than current methodologies because the former has the statistical confidence of the node that improves the likelihood of successful delivery.

In figure 7, analysis is made by comparing the proposed methodology with the traditional methodology of TSR [14] and ETRS-PD [15]at which the nodes alters from 0 (m/s) to 30 (m/s) at the maximum node.

Table 2 analysis of maximum speed vs. detection ratio (%)

Maximum speed (M/S)	TSR	ETSR-PD	Proposed
5	79	87	99
10	81.5	93	99
15	89.9	94	99.2
20	92.5	96	98.9
25	92	95	99.1
30	92	96	99

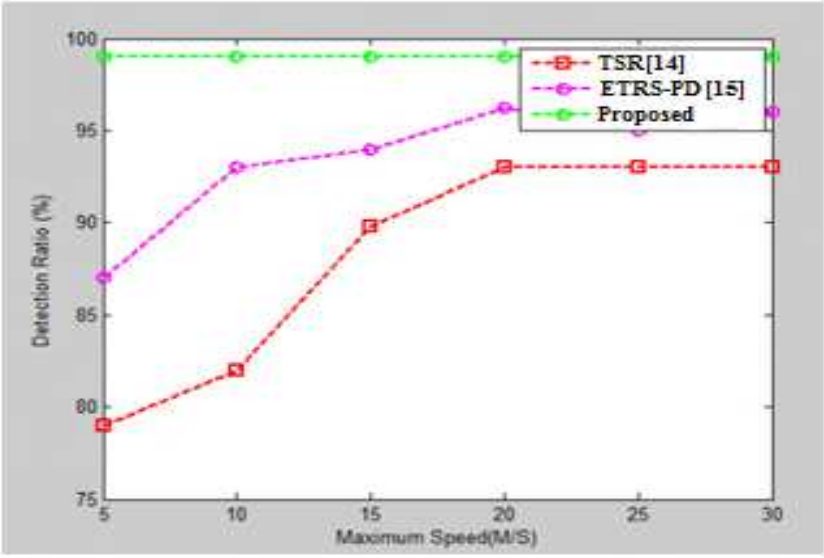

Figure 7analysis of maximum speed vs. detection ratio Ratio (%)

The nodes move more rapidly. The connections between nodes steadily increase. This means the malicious nodes have higher detection ratios. The performance of proposed technique is enhanced than the traditional approach TSR and ETRS-PD performance on behalf of detection ratio. Specifically, proposed technique has better detection ratios at higher speed.

In figure 8, the analysis is made which compares the proposed methodology with the traditional techniques TSR and ETRS-PD by varying the malicious node number.

Table 3 analysis of malicious nodes Number vs. Detection Ratio

Number of malicious node	**TSR**	**ETSR-PD**	**Proposed**
10	84	90	97
20	84.5	91	97.5
30	82.5	92.5	97.5
40	86	93	97
50	85.9	93.5	97.5

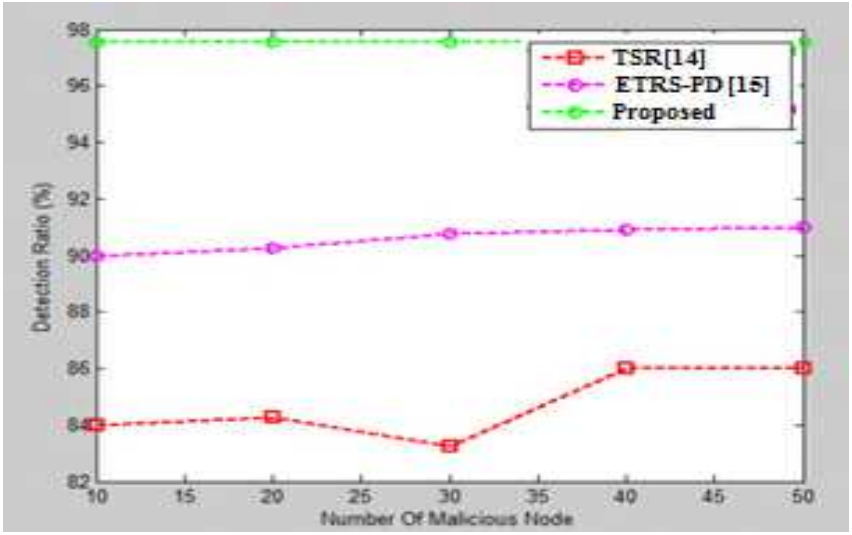

Figure 8analysis of malicious nodes Number vs. Detection Ratio

The figure 8 indicates a decrease in the proposed technique detection ratio by the rising malicious clone nodes number. It is clear that the worse nodes, serious they are further, and the more difficult they are to find. For the proposed technique, over 89% of ratios were sustained once the malicious nodes percentage is not higher than 25%. At all, proposed technique is superior to traditional methods TSR and ETRS-PD in the performance detection.

Table 4 Nodes Number vs. Rate of Successful Transaction

Number of nodes	**TSR**	**ETSR-PD**	**Proposed**
10	39	79	93
20	41	55	97.5
30	42	79	98
40	42.5	81	97.5
50	43	80	98

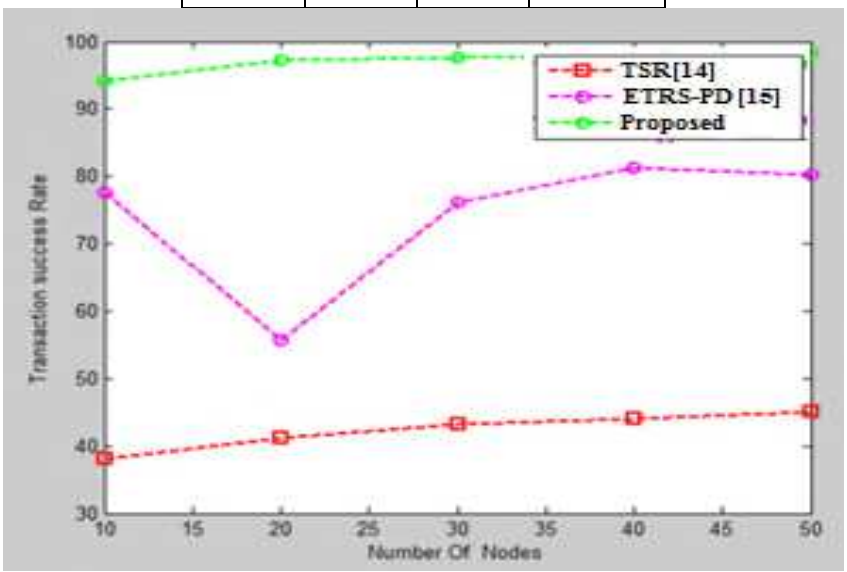

Figure 9 Nodes Number vs. Rate of Successful Transaction

Figure 9reveals the review of overall transaction success rate in an energy valuation of QoS improvement and

the identification of nodes of well-intentioned mistrust by confidence value measurement of the proposed method results in a better performance than the current approach to 30 percent. it was evident that the proposed detection technique is better and superior than the existing methodologies. Therefore, the proposed technique is proved to be an effective one on comparing other existing methods.

5. Conclusion

Routing in the communication framework is a complex task in urban environment. The routing issues will occur due to the increase mobility in the nodes. Hence because of this QoS gets decreased which is the most challenging aspect. So as to overcome the issues related to weighed-biased end-to-end delay method was introduced. Here in this paper by using the TEERP-MBHCS algorithm to find the efficient safest route within a short period. Here by using this method a shortest safest path was determined. At last, the simulation results showed that proposed technique can outperforms well in terms of node pair prediction, speed or data transfer analysis, energy consumption and bandwidth consumption that will prove the proposed method efficiency.

Declaration:

Ethics Approval and Consent to Participate:

No participation of humans takes place in this implementation process

Human and Animal Rights:

No violation of Human and Animal Rights is involved.

Funding: No funding is involved in this work.

Conflict of Interest: Conflict of Interest is not applicable in this work.

Authorship contributions:

There is no authorship contribution

Acknowledgment :

No acknowledge

References

[1] M. M. Patel and P. K. Patel, "Intrusion detection system based on trust value in wireless sensor networks," in *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2019, pp. 618-620.

[2] A. R. Dhakne and P. N. Chatur, "Design of Hierarchical Trust based Intrusion Detection System for Wireless Sensor Network [HTBID]," *International Journal of Applied Engineering Research,* vol. 12, pp. 1772-1778, 2017.

[3] T. Abdellatif and M. Mosbah, "Efficient monitoring for intrusion detection in wireless sensor networks," *Concurrency and Computation: Practice and Experience,* vol. 32, p. e4907, 2020.

[4] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, 2017, pp. 1-6.

[5] R. Khanduzi, A. K. J. C. Sangaiah, and E. Engineering, "Tabu search based on exact approach for protecting hubs against jamming attacks," vol. 79, p. 106459, 2019.

[6] J. Wang, S. Jiang, and A. O. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors,* vol. 17, p. 1227, 2017.

[7] L. Song, K. K. Chai, Y. Chen, J. Schormans, J. Loo, and A. Vinel, "QoS-aware energy-efficient cooperative scheme for cluster-based IoT systems," *IEEE Systems Journal,* vol. 11, pp. 1447-1455, 2017.

[8] W. Wang, H. Yang, Y. Zhang, and J. Xu, "IoT-enabled real-time energy efficiency optimisation method for energy-intensive manufacturing enterprises," *International Journal of Computer Integrated Manufacturing,* vol. 31, pp. 362-379, 2018.

[9] K. Kumar, S. Kumar, O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-layer energy optimization for IoT environments: technical advances and opportunities," *Energies,* vol. 10, p. 2073, 2017.

[10] N. J. I. J. o. E. Cauvery and C. Engineering, "Trust-based secure routing against lethal behavior of nodes in wireless adhoc network," vol. 10, 2020.

[11] J. Sengathir and R. Manoharan, "Exponential reliability coefficient based reputation mechanism for isolating selfish nodes in MANETs," *Egyptian Informatics Journal,* vol. 16, pp. 231-241, 2015.

[12] M. H. Ferdaus, M. Murshed, R. N. Calheiros, and R. Buyya, "Multi-objective, decentralized dynamic virtual machine consolidation using ACO metaheuristic in computing clouds," *arXiv preprint arXiv:1706.06646,* 2017.

[13] G. Swathi, "Secure data storage in cloud computing to avoiding some cipher text attack," *Journal of Information and Optimization Sciences,* vol. 39, pp. 843-855, 2018.

[14] R. Chen, F. Bao, M. Chang, J.-H. J. I. T. o. P. Cho, and D. Systems, "Dynamic trust management for delay tolerant networks and its application to secure routing," vol. 25, pp. 1200-1210, 2013.

[15] R. H. Jhaveri, N. M. Patel, D. C. Jinwala, J. Ortiz, and A. de la Cruz, "A composite trust model for secure routing in mobile ad-hoc networks," in *Ad Hoc Networks*, ed: InTech, 2017, pp. 19-45.

[16] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, and A. J. W. P. C. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks," vol. 105, pp. 1475-1490, 2019.

[17] S. Lata, S. Mehfuz, S. Urooj, and F. Alrowais, "Fuzzy Clustering Algorithm for Enhancing Reliability and Network Lifetime of Wireless Sensor Networks," *IEEE Access,* vol. 8, pp. 66013-66024, 2020.

[18] M. Ali and F. Gared, "Energy optimization of wireless sensor network using neuro-fuzzy algorithms," *Ethiopian Journal of Science and Technology,* vol. 12, pp. 167-183, 2019.

[19] D. Sharma and A. P. Bhondekar, "Traffic and energy aware routing for heterogeneous wireless sensor networks," *IEEE Communications Letters,* vol. 22, pp. 1608-1611, 2018.

[20] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. J. T. J. o. S. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," vol. 74, pp. 5156-5170, 2018.

[21] O. AlFarraj, A. AlZubi, A. J. J. o. A. I. Tolba, and H. Computing, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks," pp. 1-11, 2018.

[22] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. J. W. P. C. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," vol. 110, pp. 1637-1658, 2020.

[23] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. J. W. N. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," pp. 1-14, 2019.

[24] M. M. Mukhedkar and U. J. T. C. J. Kolekar, "Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm," vol. 62, pp. 1528-1545, 2019.

[25] M. Poongodi and S. Bose, "Detection and prevention system towards the truth of convergence on decision using Aumann agreement theorem," *Procedia Computer Science,* vol. 50, pp. 244-251, 2015.

[26] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET," *SpringerPlus,* vol. 5, p. 995, 2016.

AUTHORS BIOGRAPHIES

Putty Srividya received her B.Tech (ECE) from JNTUH and M.E (Signal Processing) from Osmania University, Hyderabad, India. She is currently working as Assistant Professor, Department of Electronics and Communication Engineering, University College of Engineering (Autonomous), Osmania University, has over 11 Years of teaching experience. She served as TPC member for International Conference CIIS 2019 to 2021. Member of IEEE and also Member of Signal Processing Society, Sensors council and Sensors Letters. Her areas of interest include Wireless Sensor Network, Signal Processing, IoT and Machine Learning

Dr. L. Nirmala Devi received her B.E, M.E and Ph.D degrees in Electronics and Communication Engineering from the Department of Electronics and Communication Engineering, University College of Engineering (Autonomous), Osmania University, Hyderabad, India. She is currently working as a Professor and chairperson Board of studies (CBOS) in the Department of Electronics and Communication Engineering, Osmania University and also Director, CHW Osmania University.She has served as TPC member organizing committee member of numerous international conferences and conducted two GAIN programs in the year 2017.She has presented her paper in IEEE flagship conference International Conference on Communications (ICC-2019) at Shanghai. She has been selected for “Outstanding Women in Engineering Award “during Annual women’s meet (AWM 2018) in the year 2018 and awarded “Best Women Researcher in Science and Technology” award in recognition of contributions to research activities in August 2021 from JNTU Kakinada in 2021. She has published many papers in various national & international journals IEEE conferences. She is also a member of IEEE, Fellow IEI and OSA.