Ingénierie des Systèmes d'Information
Vol. 29, No. 6, December, 2024, pp. 2293-2307
Journal homepage: http://iieta.org/journals/isi

Balancing Energy Fluctuations with Multi Level Trust Model for Multi Route Selection with Rank Based Route Clusters in Smart Grids

Chadalavada Naga Priyanka*, Nandhakumar Ramachandran

School of Computer Science and Engineering, VIT-AP University, Amaravati 522237, Andhra Pradesh, India

Corresponding Author Email: nagapriyankach79@gmail.com

https://doi.org/10.18280/isi.290619

Received: 11 April 2024
Revised: 29 September 2024
Accepted: 27 November 2024
Available online: 25 December 2024

Keywords:
smart grid, smart meter, power distribution, reliability, routing, trust factor, multi route selection, route clusters

ABSTRACT

A smart grid is a power distribution network that utilizes information and communication technologies to manage, track, and direct the flow of information between power generators and consumers. Only with dependable communication networks can a smart grid provide a wide range of electrical services while simultaneously streamlining and optimizing energy consumption. In a smart grid network, the Advanced Metering Infrastructure (AMI) sensor nodes detect, analyze, and communicate data; all of this activity necessitates energy, a finite resource that is crucial for the network's upkeep over time. Wireless mesh networks have the same trust issues that plague conventional distributed ad hoc networks. The proposed model considers the multi level trust models for the nodes for mitigating energy fluctuations. This research considers an Energy Efficient Multi Level Trust Model for Multi Route Selection with Rank based Route Clusters (EEMLTM-MRS-RRC) in Smart Grid that maintains multiple routes by considering the trust factors. The proposed model calculates the trust factor of nodes in smart grid by considering the internal and externals factors. The proposed model selects a cluster head node for analyzing and monitoring the internal and external factor of nodes in the network. The proposed model achieved 98.5% accuracy in Energy Consumption Reduction and 98.6% accuracy in Trusted Route Selection. The proposed model, when contrasted with traditional routing models, performs better in energy consumption reduction and route maintenance.

1. INTRODUCTION

Incorporating smart devices into the conventional grid allows for automated monitoring and control, as well as two-way communication across systems known as the Smart Grid (SG) [1]. Like the conventional grid, the SG relies on distribution, transfer, and generation to function well. The establishment and ongoing development of the smart system is made feasible by the integration of the cyber infrastructure with the physical components of the traditional power systems [2]. Electric vehicles, energy from renewable sources, and various distributed power generators are just a few examples of the varied uses and integrations made possible by the Smart Grid [3].

Smart grid refers to an electrical network that tracks and manages the flow of power from power plants to homes and businesses using digital technologies [4]. Because it uses a wide range of Information and Communications Technology (ICT), it considerably improves the current electrical infrastructure. The goal is to make power distribution more efficient, less wasteful, and more responsive to changes in demand.

In order to carry out their sophisticated functions, smart grids rely on a number of essential components:

Smart Meters are devices that allow utilities and consumers to track power consumption in real-time. Users are able to make better judgments regarding their energy consumption using the data they supply on trends of energy usage.

Integral to the smart grid are sensors and monitoring systems, which record information about energy flows, grid infrastructure health, and possible interruptions or outages.

To improve operational efficiency and enable demand response capabilities, a system is needed to measure and analyze energy usage data in real-time. This system is known as AMI.

Timely reactions to changes in energy demand or generation are ensured by robust ICT infrastructures that allow the secure transmission of data across different grid components.

Technologies that produce energy on a smaller scale and add to the grid's overall energy mix are known as distributed energy resources (DER).

Security of the Smart Grid is crucial because of the increased attack vector introduced by the cyber infrastructure's incorporation into the SG. As a result, studies have been conducted on subjects like routing, encryption, cryptographic key generation and management [5], privacy, risk assessment and trust of the nodes in the network. The level of trust inside the SG is crucial for determining the legitimacy of a given activity, transaction, or communication [6]. Devices attacked with malicious actions can be benefited from the use of trust in order to verify the safety of malicious commands before acting on them [7]. Next-generation electrical power systems, or SGs are becoming increasingly popular because of the intelligence and efficiency they provide to the power grid [8]. Two-way communication between utilities, electrical devices, and software relies on a highly available network [9]. The availability of the smart grid communication system can be ensured by the use of redundant routes provided by the wireless mesh network technology. It is also a promising solution for smart grid because of its great degree of adaptability and scalability [10].

The smart grid's stability is at risk due to rising electric demand and the increasing incorporation of renewable energy sources. A number of approaches aimed at regulating demand rather than boosting the supply's spinning reserve have been put forward as potential solutions to the energy fluctuations problem. Here, we zero in on dynamic demand control, a way that smart devices can self-adjust their operation schedules based on the electric frequency. The necessity to recover outstanding work raises the likelihood of big demand peaks, and hence huge frequency fluctuations, even though conventional control techniques can successfully mitigate small and medium size frequency fluctuations. Strategies to prevent these occurrences should be considered since, despite their rarity, they have the ability to cause the system to fail.

Two-way communication between electrical utilities, electrical units, and electrical applications is made possible by the Smart Grid, a trend of the future generation electrical power grid. Market, customer, service provider [11], bulk generation [12], dispersion [13], operation, and transmission are several areas in which the Smart Grid standard is defined by the National Institute of Standards and Technology (NIST) [14]. Using data control transmission, the Smart Grid communication network anchors and links these domains together to enable interactive operation, with the ultimate goal of optimizing energy usage across power grids [15]. Smart Grid is the combination of the current electricity grid with the information and communication technology [16]. When it comes to supporting interactive operations among electrical services and applications, the communication network takes on increasing importance in the Smart Grid. With built-in reliability and durability in its topology, low-cost scalability [17], and flexibility [18], wireless networks are a viable infrastructure for Smart Grid. Packet latency and packet loss both rise when a network is experiencing attacks and other forms of instability. Since every action in a communication network requires energy [19], this would result in a net increase in the amount of power needed to accomplish the same task [20].

Combining smart grid technology with the Internet of Things had many advantages that are:

Enhanced Energy Efficiency: Smart grids make it possible to distribute and use energy more efficiently, which means less wasted energy and lower consumption overall.

Enhanced Security Levels: Smart grids' ability to detect and react to attacks in real time enhances security, which in turn helps to protect vital infrastructure.

Highly Scalable: The digital aspect of smart grids makes it easier to include renewable energy sources and future technologies, making them scalable and adaptable to shifting energy landscapes.

Reduced Operating Expenses: Smart grids help utilities save money on operations by improving efficiency and cutting down on outages. This savings is then passed on to consumers as cheaper energy pricing.

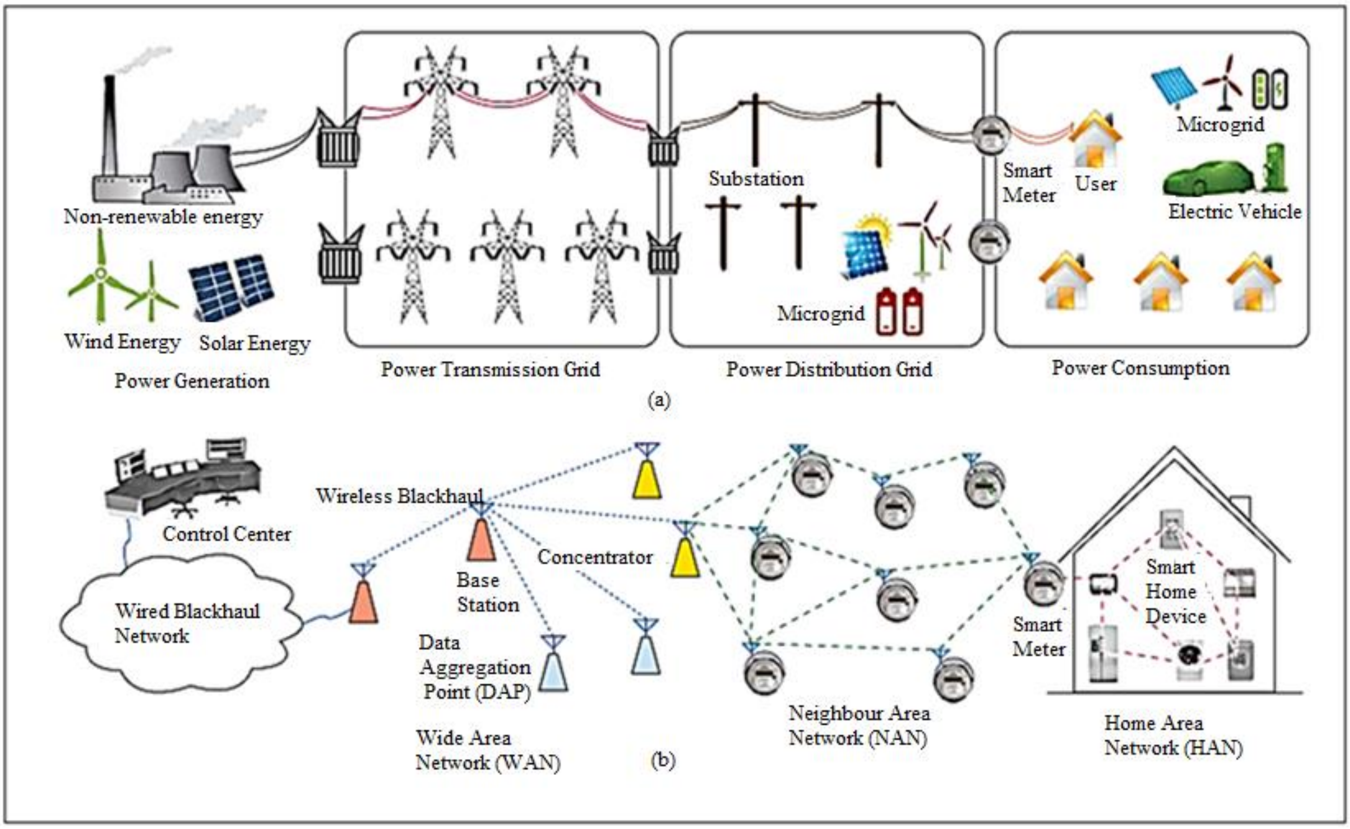

Figure 1. Complete SG layers architecture [19]

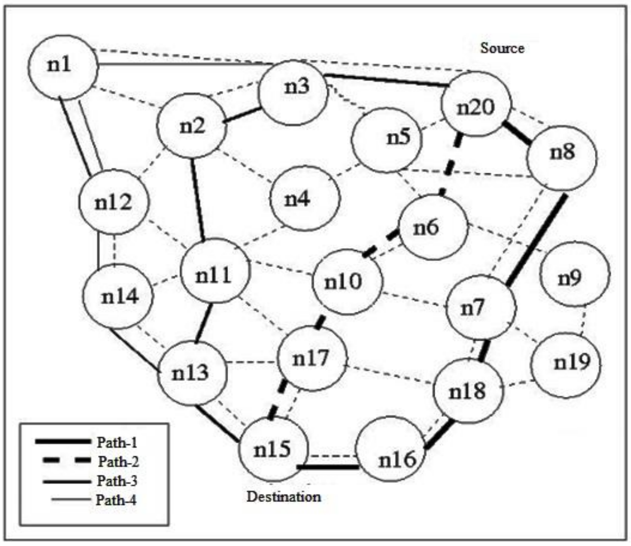

Figure 2. SG routing model [20]

While the Smart Grid has great potential as an energy-saving solution, the communication network's interactive operation and control will result in significant energy consumption [21]. To address these vulnerabilities and to improve energy efficiency by protecting against packet loss and long latency, a trust- based multi routing protocol is proposed that avoids delay in the smart grid in case of routing issues [22]. The proposed model is more effective in large wireless networks because it employs node trust information and selects the best routes with minimum energy consumption. Despite the presence of potential threats, SGs must still complete the task of transmitting data from one node to another throughout the network. Unpredictable environmental behavior, shifting network topologies, and shaky communication can all play a role in disrupting network services.

SGs adaptability makes it useful in a wide range of settings. While different applications have varying needs for Quality of Service (QoS) parameters including throughput [23], energy efficiency [24], delay, etc., security is always a top priority. The characteristics of a program are the main factor in determining its safety [25]. However, smart networks require distinct approaches to security from those used in traditional, infrastructure-based networks. Furthermore, the features and QoS factors of each application domain are different. While multipath routing uses many paths to provide connectivity in the event of a link loss [26]. Additionally, route discovery is not always triggered when a link fails in a multipath routing system [27]. This is because, for small values of route 'R', the network is fault tolerant, meaning that the disruption of network services is not caused by a single failed connection [28]. The complete architectural layers of SG are shown in Figure 1.

Multiple control systems and appropriate management including demand forecasting, technical maintenance, generation and transmission planning, etc. form the basis of the smart grid's steady operation. System operators have the critical responsibility of controlling the grid frequency to guarantee the grid's efficiency, dependability, and stability on a worldwide scale. A healthy supply-and-demand relationship between power generation and load/power consumption is crucial for frequency regulation. The frequency will increase if the supply is greater than the load, and it will decrease if the reverse is true. Because of the unpredictable nature of the load and the growing fluctuations of the supply as a result of renewable energy sources' incorporation, striking this equilibrium is challenging. Extra big fluctuations could be introduced if power lines go down or if a power plant fails. Therefore, conventional operation adjusts the supply side in response to a power imbalance by adjusting it to match the load. This necessitates that smart grid possess additional generation capacity, often known as spinning reserve, which enables them to adapt the power output in response to changes in frequency. In addition, standard grids use supplemental or non-spinning reserves that are connected to quick-response generating units that may be turned on in a matter of minutes.

Although the terms are sometimes used interchangeably to refer to a risk-free system, distinguishing between trust and security is crucial to understanding the concept of trust. Trust between nodes is typically measured as an evaluation of the other nodes' dependability. As a result, it is important to employ measures beyond trust to keep networks safe. When it comes to SGs, there are a wide variety of behaviours that are considered malicious. As a result, the SGs needs a reliable method of discovering security issues [29]. Malicious nodes in SGs are able to successfully switch between states and launch attacks on the network's resources because of the nature of nodes participation in the communication. Therefore, it is crucial to maximize efficiency to choose which nodes will participate in the data transmission. Trust models are a solid method for accomplishing this goal. Models like this can aid nodes in detecting harmful activity and making the right choices [30]. The trust-based routing models in SG is shown in Figure 2.

Limitations in areas like power, storage, memory, and computation have led to the discussion of how to quantify node trust [31]. Because of this, it is crucial that scalable trust models be made available that account for these constraints. In this research, a decentralized trust model in which nodes employ both direct and indirect measures of trust is considered, and where no node keeps any trust values other than those of its neighbours. Therefore, the model's reproducibility is enhanced by this method of trust and distribution measurement. Nodes cluster for a variety of reasons, including proximity to one another and energy levels [32]. Another crucial consideration is the degree of trust. To enhance SGs security, it is crucial to provide an energy-aware trust mechanism with low complexity and overhead. Bayesian analysis is generally used for establishing route in networks. Using probability statements, Bayesian analysis provides answers to research issues involving unknown parameters. Bayesian analysis fails to disclose which node should be chosen as a routing priority. The ability to convert one's own personal set of beliefs into a formalized mathematical prior is crucial for performing Bayesian inferences. The inference procedure of the model may take some time. If there is a large amount of available data for smart grid node data, the Bayesian strategy is not worthwhile, and the regular probability approach can accomplish the work more efficiently. The proposed methodology employs the Enhanced Maximum Likelihood Estimation technique to compute the direct and indirect trust of smart grid nodes. The estimators of the shape-scale node parameters were derived using the enhanced technique. This research considers an EEMLTM-MRS-RRC in Smart Grid that maintains multiple routes by considering the trust factors. The main contributions of this research are:

- We proposed a novel trust calculation model that calculates the direct and indirect trust calculation of each node in SG using Enhanced Maximum Likelihood Estimation model. To do this, we maximize a likelihood function so that the observed data of a node is the most probable for picking that node into the routing process, given the stated statistical model. The estimators of the shape-scale family parameters were derived using the enhanced technique and compared to Bayesian estimators depending on the informational and kernel priorities.

•We designed a model for selecting network head evaluator node among the trusted nodes. The Manhattan distance model is used to calculate the distance among the trusted nodes and node that is nearer to the threshold number of nodes is considered as an evaluator node.

•The nonlinear knapsack problem is applied on the trusted nodes to select the best trusted nodes by ranking them and Trust Linked Probabilistic Controller (TLPC) is applied to select the multiple trusted shortest routes in the network for improving the network reliability during link issues.

2. LITERATURE SURVEY

The Industrial Internet of Things (IIoT) is useful for a wide variety of industrial tools and machinery, including robots, medical equipment, and SDM systems. Although the IIoT has great promise, there is room for development in the following areas: connectivity, security, privacy, heterogeneity, scheduling, and energy consumption of the networks. The intermittent nature of the nodes and the widespread use of IIoT has reduced the lifetime of the networks and introduced energy-limited units into them. It is also believed that the best approach to address the privacy and security issues raised by the IIoT design is to use safe routing algorithms. For a cluster-based IIoT environment, Nagappan et al. [1] proposed a method called TAMOMO-SCRP, which stands for trust-aware multiobjective metaheuristic optimization based secure clustering with route planning. The TAMOMO-SCRP approach, proposed for use in routing and clustering, is mainly concerned with the creation of bald eagle search (BES) algorithms.

For transportation planning to be intelligent, a trustworthy and safe transportation service is essential. In order to curb the wasteful consumption of computer resources, Li et al. [2] implemented and improved the trust model. In addition, the author introduced a Trusted Parallel Optimization on Route Planning (T-PORP) that utilizes a Dual-level Grid (DLG) index. This optimization method enables users to continuously handle the route planning process in parallel. The author periodically estimated road weights taking into account the ever-changing traffic conditions using a Long Short-Term Memory (LSTM) neural network.

There are already billions of connected devices and smart things in use, and that number will only grow. Encryption and protection are prerequisites for the transmission of the vast quantities of data produced by IoT devices over the network. Certification bodies allow users to confirm the legitimacy of a node in a network by linking its public key to its self-reported identity. Hameed et al. [3] proposed utilizing blockchain technology. The suggested method for managing keys and trust in IoT networks is shown to be scalable by the presentation of an effective proof-of-concept. The proposed approach is evaluated by measuring the throughput and the access time delay.

A dependable service provisioning method for Safe-as-a-Service (Security as a Service) infrastructure in IoT-based ITS was proposed by Dass et al. [4]. Decision virtualization is a common approach used by Safe-as-a-Service platforms to make personalized safety-related decisions in real-time, allowing them to meet the demands of their numerous customers. The author considered the transportation sector as a potential setting for Software as a Service (SaaS) to enable trustworthy decision-making. However, the dependability of the data channel and the confidentiality settings of all involved sensor nodes impact the efficacy and accuracy of the subsequent judgments. The author laid up a framework for evaluating trust in order to ascertain the veracity of the data generated by these nodes.

Quality of Experience (QoE) enhancement routing (QER) was introduced by Li et al. [5] as a smart protocol based on collaborative theory. Prior to delving into the possible applications of MWN, a comprehensive examination of the key factors influencing the data transmission procedure is offered. In order to find the optimal routing strategy based on real-time network data, the QER protocol uses two steps: collaborative observation and smart decision. Detailed procedures are provided that correlate to the capabilities of the system. Third, in order to compare and contrast their performance, the author included three distinct routing mechanisms into QER. In order to conduct tests, realistic settings are established. The system was able to intelligently execute the optimum strategy according to the outcomes of these performance tests.

Elastic optical networks (EONs) are an exciting new optical technology that could revolutionize the way the Internet handles data transfer and connectivity in the future. This is especially true when thinking about how ideas like the Internet of Things (IoT), the Tactile Internet, and Industry 4.0 will impact this landscape. Each optical circuit or light path is independently furnished in this network design by use of superchannels with configureurable bit rates. Following a review of relevant literature, Ruiz et al. [6] introduced multi-path best-fit (MP-BF), a novel RMSA method that leverages EONs' adaptability through the integration of a spectrum assignment technique with a split-spectrum multi-path strategy.

3. PROPOSED MODEL

The SG is an advanced electrical distribution network. Its advanced communication capabilities can boost system efficiency, reduce energy use, and ensure consistent service delivery, and network integration is a key component [33]. The routing protocol is a major challenge in the development of SG's communication networks because of the specifics of the deployed environment and other SG characteristics. Home area networks (HANs) and neighborhood area networks (NANs) are two types of networks that make up the smart grid's communication backbone, and they were the focus of extensive analysis of routing protocols [34]. HAN protocols can be broken down further into those that employ wireless communication. The Medium Access Control (MAC) protocols they use determine how they are built, how much they cost, and how fast they can move data [35]. Application needs, such as those for dependability, security, and quality of service, are taken into account when classifying routing protocols for NANs in addition to the underlying communication used for routing.

The AMI application's unique routing protocols have attracted a lot of attention from researchers; these protocols pose the biggest threat to the smart grid's NAN usage. The Internet of Things (IoT) has emerged in several sectors in the last several years, including transportation, healthcare, and even academia. The Internet of Things (IoT) integrates several services to achieve its goals [36]. The goal of these services is to give consumers convenient, personalized experiences through smart actions that connect their devices to the physical environment. Because of the tremendous advancements in modern technology, attacks have grown increasingly common and complex. Malicious actors sometimes exploit the diversity of the Internet of Things (IoT) to cause confusion among consumers regarding the reliability and safety of their connected devices, as well as the service they provide. Trust is thus a security concern for IoT smart services.

To identify questionable behaviour and distinguish between harmful objects, trust management strategies have been widely used in recent years. Nevertheless, these technologies still have a way to go before they can fully address complex problems, such as dealing with large amounts of data or unpredictable behaviours. Security is a top priority in SG-based communications because of the large range of linked devices. This study presents a novel trust-assuring approach that considers a broad variety of contextual parameters, including the interactions between individual nodes and their power states, in response to the challenges of SG network security. It is also advised to use a minimum hop count approach to select a route that requires the least amount of processing time. This study develops a composite routing metric that considers all of these criteria when determining which node to employ as the subsequent link in a communication chain. As a method for improving security, trust management helps protect data and user privacy. Verifying the trustworthiness of nodes before granting them permission to request help is crucial for SG security.

The distribution of fluctuations' probabilities changes, with huge tails introduced, due to the need to recover outstanding work. Consequently, even though the energy balancing model is effective in decreasing small and medium size fluctuations, the likelihood of uncommon occurrences causing big frequency variations becomes non-negligible. An unsafe unforeseen effect of small-level load balancing could cause the smart grid to go down. Afterwards, methods to prevent such unintended consequences must be considered. In this research, proper communication between smart devices, either directly or via a hub, is an easy way to minimize or eliminate excessive frequency variations caused by the necessity of recovering unfinished tasks is considered. In contrast to other efforts, the suggested method is primarily concerned with coordinating the switching of various devices in order to maintain a constant cluster power consumption through the exchange of very little data.

The node in need of assistance checks the reliability of its neighbours before passing information along to them. The fundamental issue with current trust definition approaches is that they do not easily allow for the development of metrics and evaluation frameworks. The challenges of identity administration and access control are also directly tied to the criteria of satisfaction or trust. Taking into account the multifaceted technique to evaluate the trustworthiness of SG nodes, this research provides a novel trust-aware routing framework for SG networks. To describe a node's trustworthiness in an SG network, the multi-level trust approach took into account both its communication trust and its energy trust. Additionally, multiple paths are picked based on the hop count for a given source and destination node pair. The suggested method is resilient against resource limits and security constraints since it takes into account multiple variables in choosing a forwarding node. Whereas traditional methods only addressed one of these two issues, energy or security, at a time. The proposed model architecture is shown in Figure 3.

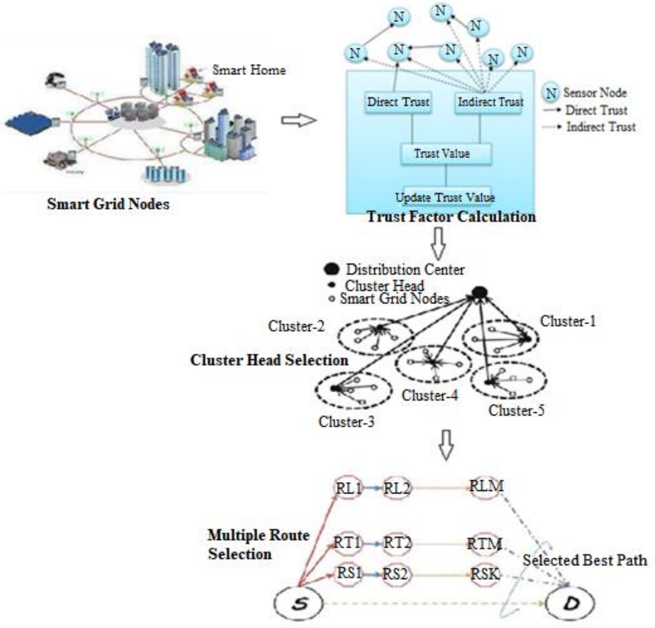

Figure 3. Proposed model architecture

A control system that reduces the frequency stability impact of electric power on the grid could be an asset to a smart grid. For lower electric supply, the smart grid can control load. When called upon, the smart grid may regulate the amount of electricity generated by renewable sources. While auxiliary appliances aren't required for load balancing applications, power losses can happen based on factors including energy fluctuation amplitude, smoothing level, and frequency of balanced power fluctuations. To lessen the fluctuations, trusted nodes are considered and clusters are generated. Ranks are allocated to the clusters for the effective load balancing in the selected route.

There are a number of benefits to using Manhattan distance and the nonlinear knapsack problem (NKP) for smart grid route selection. While NKP is great at improving resource allocation and satisfying different constraints, Manhattan distance is great at computing efficient routes in grid-like systems. Utilizing these approaches can greatly improve smart grid solutions, which in turn improve operational efficiency and electricity distribution dependability.

Because it is both simple and computationally efficient, Manhattan distance is ideal for use in smart grid route selection. Since most urban infrastructure only allows for horizontal and vertical mobility, this metric—which measures the distance between two places in a grid-like pattern—works wonderfully with it. Smart grid systems can find the quickest routes for distributing energy by using Manhattan distance, which reduces travel time.

One area where the nonlinear knapsack problem shines is in smart grid route selection optimization for resources. To maximize energy savings while limiting operational expenses, for example, are two examples of nonlinear constraints and goals that NKP excels at handling. Because smart grids must frequently weigh opposing concerns like cost, environmental effect, and dependability, this capacity is crucial.

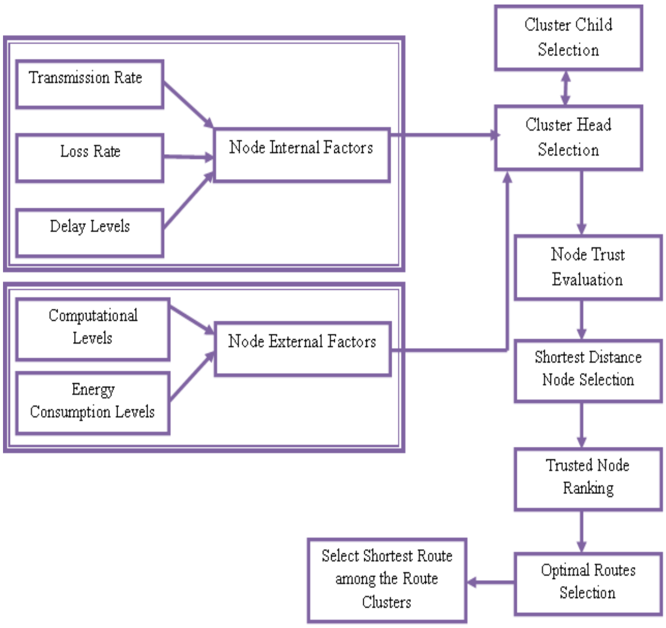

Figure 4. Proposed model workflow

Table 1. Notations

Notation	Description
Δ	Packets Received
Λ	Packets Sent
Β	Packet Delivery Rate
Γ	Energy Allocated
Τ	Energy Consumed
Α	Transmission Rate
μ	Delay Level
Ω	Loss Level
N( )	Smart Grid Node
Σ	Computational Level
N	Current node
M	Total Nodes in SG
Th	Threshold Value
Ξ	Time Instant
DT	Direct Trust
IDT	Indirect Trust
Π	Maximum Likelihood Estimator
TF	Trust Factor
NC	Node Capabilities
T	Manhattan Distance
RS	Route Selection
φ	Route Ranking

For smart grids to function properly, the supply and demand for electricity must be constantly tracked. Smart grids can make rapid modifications to power generation and transmission techniques to preserve energy balance with the use of energy demand forecasting models, which estimate future loads and energy supply. Smart grids face difficulties with the unpredictability and unreliability of renewable energy sources. The proposed model flow of work is shown in the Figure 4.

The smart grid node's own perception in unrestricted mode is the basis for a direct trust relationship. In a wireless network, a node can interact directly with any other node and receives any traffic within its radio range regardless of how the data was originally routed. In the smart grid network, an indirect trust relies on the other node or recommender for communication. With indirect trust, one node contacts another via the network's recommender nodes. This trust model illustrates indirect trust by demonstrating how to communicate with smart grid nodes that have already been installed throughout a network. The node trust calculation algorithm calculates trust of each node by considering the internal and external parameters. The notations represented in the proposed mathematical models are indicated in Table 1.

Algorithm Node_Trust_Calculation

{

Consider a smart grid SG that contains nodes $\{SGN_1, SGN_2, \ldots, SGN_M\}$. The energy γ is allocated to the smart grid.

The nodes information in the network will be gathered and processed. The nodes data will be maintained by the network authority. The node information is used to communicate with the node and also to monitor the nodes in the network. The node information processing is performed as

$$NR[M] = \sum_{n=1}^{M} phyaddr\big(N(n)\big) + \frac{\tau(N(n))}{\gamma} + \alpha + Th$$

A trust value will be assigned to each node in the network that processes data. Packet transmission ratio, end-to-end delay, throughput, and normalized routing overhead are some of the metrics used to determine a node's trust factor. The calculation of the trust factor will involve determining the nodes' direct and indirect trust. The direct and indirect trust of the nodes are calculated as

$$TransmissionRate(\alpha)[M] = \sum_{n=1}^{M} \frac{\lambda(N(n))}{\omega(N(n))} + \alpha(N(n))$$

$$LossRate(\omega)[M] = \sum_{n=1}^{M} \lambda(N(n)) - \delta(N(n))$$

$$DelayLevel(\mu)[M] = \sum_{n=1}^{M} \xi(\lambda(N(n))) - \xi(\delta(N(n)))$$

$$DirectTrust\ (DT)[M] = \prod_{n=1}^{M} \frac{\delta(N(n))}{\lambda(N(n))} - \frac{\sum_{n=1}^{M} \beta(N(n)) * \delta(N(n))}{\lambda(N(n)) * \xi(\lambda(N(n))}$$

$$IndirectTrust(IDT)[M] = \prod_{n=1}^{M} \frac{\sigma(N(n))}{M} * (\gamma(N(n)) - \tau(N(n)))$$

In order to determine a node's ultimate trust degree levels, the proposed method use the Enhanced Maximum Likelihood Estimation model for both direct and indirect trust calculations within the smart grid. Enhanced maximum likelihood estimation can be employed to estimate the requirements of an assumed probability distribution using some observed data from smart grid nodes. This is accomplished by maximizing a probability function such that, according to the specified statistical model, the information that is observed of a node is most likely to be used to select that node for the routing process.

The likelihood function LF(ε; M) for M node sin the smart grid contains the data to be transmitted and unknown attributes in the network is represented as ŋ=(λ, δ) and the data packets {dp_1,dp_2,….,dp_L}. The maximum likelihood estimator (ϖ)is represented as

$$\frac{dx}{dy}(M) = \sum_{n=1}^{M} F(ŋ,\lambda) + \max(DT) + \max(IDT) + \frac{\alpha}{\omega} withtheinitialnodeconditionasŋ(\delta) = \max(\alpha)$$

The enhanced maximum likelihood estimation is performed to calculate the final trust value as

$$\overline{\overline{\frac{dx}{dy}}}(M) = \sum_{n=1}^{M} \max\,(\frac{dx}{dy}(n)) + F(ŋ,\delta) + \frac{\max(DT)}{\min(DT)} + \frac{\max\,(IDT)}{\min\,(IDT)}$$

$$TrustFactor(TF)[M] = \sum_{n=1}^{M} \max\,(\overline{\overline{\frac{dx}{dy}}}(n))$$

A DT and IDT based trust estimation is one that is more than threshold 0.5, where trust values typically range from 0 to 1. If the nodes trust values sum to 1, it has the highest level of trustworthiness possible. If a device's estimated trust value is below 0.5, it is seen as displaying selfish conduct or being malevolent; devices with trust ratings below 0.3 are flagged as potentially harmful. If a device's trust score is zero, it is the most malevolent device, exhibiting the worst possible behavior or generating the greatest possible number of packets, hence posing an unlimited flood threat to the network.

The energy consumption levels of the nodes with their trust values are calculated. The energy consumption of the nodes is calculated based on the node capabilities. The node behaviour will reflect the energy consumption levels. The energy consumption levels of each node are calculated as

$$EnergyConsumption(\tau)[M] = \sum_{n=1}^{M} [\gamma\big(N(n)\big) + \tau\big(N(n)\big)] * \alpha(N(n))$$

}

Psecudocode: EEMLTM-MRS-RRC

```
γ=100MW
α=100mbps
Trth=70mbps
Th=30
Counter=1
Rank=1
Rth=80
Trust TTh=75
Disth=25
Dth=10ms
NCth=50
ITh=65
Msg[M]=getData($SG_{set}$)
For each node $SGN_i$  in $SG_{set}$
For i in $SG_{set}$
addr[i]=phyaddr($SGN_i$)
τ=ener($SGN_i$)
re=γ($SGN_i$)-τ($SGN_i$)
Nodereg[i]=addr[i]+τ[i]+re[i]
i=i+1
End for
For j in $SG_{set}$
α[j])=δ(j)-ω(j)+α(j)
loss[j]=λ(j)-δ(j)
For k in $SG_{set}$
IV=δ(j)/λ(j)
DT[k]=IV-
For f in range(k)
DT[f]=IV(k)-((β(k)*δ(k)/ξ(k)*λξ(k))
IK[f]=σ(k)/range($SG_{set}$)
IDT[f]=IK(f)*(γ(k)-τ(k))
f=f+1
k=k+1
end for
j=j+1
end for
i=i+1
end for
For each node $N_i$ in $SG_{set}$
If ((DT($N_i$)>=75) && (IDT($N_i$)>=65))
NodeTID=1
else
NodeTID=0
i=i+1
End for
For each node H in $SG_{set}$
if($ŋ(\delta) == \max\,(\alpha)$)
MLF[H]=max(DT(H))+max(IDT(H))+(α/ω)
Tf[H]=(max(DT)/min(DT))+(max(IDT)/min(IDT))
Ener[H]=(γ(H)+τ(H))*α(H)
H=H+1
End for
For each node $N_i$ in $SG_{set}$
If((α($N_i$)>=Trth) && (ω($N_i$)<0.5))&&(μ($N_i$)<dth)
NC[$N_i$]=counter
Else
NC[$N_i$]=0
Counter=counter+1
i=i+1
End for
For each node $N_i$ in $SG_{set}$
For i range ($SG_{set}$)
For j in range(i)
ManHD[$N_i$]=(j+1-j)/(i+1-i)
If((ManHD($N_i$)<disth)&&(NC(i)>NCth))
NHEN[$N_i$]=NodeTID($N_i$)
i=i+1
j=j+1
End for
End for
End for
For each node $N_i$ in $SG_{set}$
For i range ($SG_{set}$)
For j in range(i)
If(ManHD($N_i$)<disth)&&(NC(i)>NCth))
If(((α($N_i$)>=Trth) && (ω($N_i$)<0.5))&&(μ($N_i$)<dth))
Rank($N_i$)=Rank
```

```
If(Rank($N_i$)>=Rth)
RS[i][j]=NodeTID($N_i$)(i)(j)
Else
Continue
Rank=Rank+1
i=i+1
J=j+1
End for
End for
End for
End for
```

The proposed approach chooses a node to act as the Network Head Evaluator Node (NHEN), keeping monitoring on everything and pinpointing the safest possible path through the network. The Manhattan distance is used to determine the top dog smart grid head node. The Manhattan distance is a standard unit of measurement that adds together the x and y separations between points. The proposed model performs ranking of trusted nodes in the SG. Nonlinear knapsack problem is used to rank trusted nodes. The knapsack problem is a combinatorial optimization problem in which one is given a set of nodes, each of which has a weight and a value, and one must choose which nodes to include in the routing process so that the sum of the weights is less than or equal to a given limit and the sum of the values is as large as possible while still only including trusted nodes.

Algorithm NHEN_Selection

{

The trust factor of each node is calculated and based on the trust factor, based on energy consumption, the nodes capabilities are calculated. The individual node capabilities are calculated as

$$NodeCapabilities(NC)[M] = \sum_{n=1}^{M} getattr\big(NR(n)\big)$$

$$NC \leftarrow \begin{cases} NC \leftarrow \max\,(\alpha\big(N(n)\big) + \min\,(\omega\big(N(n)\big) + \min\,(\mu(N(n)) & \\ NC \leftarrow 0 & Otherwise \end{cases}$$

The node distance with other nodes is calculated using the manhattan distance and the node which has nearer distance to maximum nodes in the trusted node set is considered as NHEN node. The manhattandistance of nodes is calculated among 2 nodes SGN_i and SGN_j that are in the location points (SGN(X1), SGN(Y1)) and (SGN(X2), SGN(Y2)) as

$$ManhattanDistance(\text{ƭ}) = \sum_{n=1}^{M} \frac{\sum(X2 - X1)}{\sum(Y2 - Y1)} \\ +|SGN(X_n) - SGN(X_{n+1})| \\ +|SGN(Y_n) - SGN(Y_{n+1})|$$

The proposed model selects a node from the available trusted nodes a network head evaluator node. This NHEN is selected from the trusted nodes which has the highest capabilities. The NHEN node selection is performed as

$$NHEN[M] = \sum_{n=1}^{M} \frac{\max\,(NC\big(N(n)\big))}{M} + \min\,(SGN(\text{ƭ}))$$

$$\begin{cases} \text{ƭ} \leftarrow \min\,(NC(\mathrm{GN(X1), SGN(Y1)}) \\ \quad continueOtherwise \end{cases}$$

}

In this research, a Trust Linked Probabilistic Controller (TLPC) model is used to find multiple minimum-distance routes that include only trusted nodes. This research proposed an EEMLTM-MRS-RRC in Smart Grid considering all the factors that maintains multiple routes by considering the trust factors. The proposed model is divided into three modules. Initially the node t rust calculation algorithm is implemented for processing node information and the node trust calculations are performed. After trust factors are calculated, the NHEN selection is performed that monitors the entire network. Finally, the TLPC module selects the best minimal distance trusted route and energy consumption levels are calculated.

Algorithm Trust_Linked _Probabilistic_Controller

{

The distance-based route selection process is performed that is used for communication. The distance-based route selection process is performed as:

$$Rselection(RS)[M] = \sum_{n=1}^{M} \max\big(NR(n)\big) \\ +\min\,(\text{ƭ}(N(n), \text{ƭ}\big(N(n+1)\big) + \min\,(\tau\big(N(n), N(n+1)\big))$$

$$RS \leftarrow \begin{cases} RS[\quad] \leftarrow \max(\alpha) + \max(DT, IDT) + \min(\omega) \\ \qquad + \min(\text{ƭ}) + NHEN(N(n)) & \\ continue & Otherwise \end{cases}$$

The selected routes based are distance is considered for final selection for multiple routes. The Nonlinear knapsack problem is used to rank the selected routes. The process of route ranking is performed using nonlinear knapsack problem with nodes count N_i (max) with a probability function $Prob_f$(max) is performed as

$$Prob_F[M] = \prod_{n=1}^{M} max \left\{ \sum_{n=1}^{M} RS_n \right. \\ * N_n | \sum_{n=1}^{M} [\min(\omega) + \min(\tau)] \geq Th$$

The nonlinear knapsack problem is represented as

$$\mathrm{NKP[M]} = \max \sum_{n=1}^{M} Prob_F(\delta, \lambda) * \sum_{n=1}^{M} \max\,(Prob_F({}^{\varphi}, \sigma)$$

$$RouteRank({}^{\varphi}) = \sum_{n=1}^{M} \frac{Max(NC(n, n+1))}{M} \\ + \frac{\max\big(NKP(n)\big)}{\max(Prob_F)} + \max\big(RS(n, n+1)\big) + \max(DT) \\ + \max(IDT) + \min\,(\tau(n, n+1))$$

Step-3: The TLPC model is applied on the selected routes based on ranks. The proposed model considers minimum distance routes that include only trusted nodes. The multiple route selection process is performed as:

$$MRS[M] = \sum_{i=1}^{M} \sum_{j=1}^{M} selecRoute\,[i][j](\max({}^{\varphi}))$$

$$MRS \leftarrow \begin{cases} MRS[i][j] \leftarrow \max({}^{\varphi}) + \max\big(NKP(n)\big) + \\ \quad \max(Prob_F) + \min(\text{ƭ}) \\ \quad continue \qquad Otherwise \end{cases}$$

}

4. RESULTS

Trust is an intangible concept whose meaning changes over time and across contexts, influenced by both concrete and intangible factors. Because of this, it is clear that trust is a multifaceted notion that encompasses many other qualities besides only trustworthiness. Therefore, trust management is more difficult than security itself, especially in the developing sector like IoT. Trust in SGGG is shorthand for investigating the actions of connected nodes. The history of reliable communication between two technologies shapes how they interact in the future. When nodes have trust in one another, they're more likely to work together cooperatively. To make smart choices in setting up dependable and efficient communication between devices, trust management facilitates the computation and analysis of trust among SG nodes.

Problems with trust in the SGs can be mitigated with careful trust management. Such approaches have been used to enhance security, facilitate decision-making, detect malicious activity, quarantine harmful objects, and reroute their functions to safe areas. Researchers have devised a number of methods to address trust difficulties. Problems that these solutions have to deal with include the dynamic and heterogeneous nature of SGs, the large amounts of data it generates, the high energy it consumes, the difficulty of quantifying uncertainty for untrusted behaviours, and the difficulty of selecting the optimal trust model components. In this research, a novel trust evaluation mechanism is proposed for selected the multiple trusted nodes in the SG to achieve secure data transmission. At the same time, it mitigates the risk of being misled by hostile nodes during the trust assessment procedure by utilizing network-related factors like the frequency of communication and the likelihood of successful data transmission. In this case, direct and indirect measures of trust in communication are considered.

Grid frequency energy stability is under increasing strain from the increasing penetration of renewable resource energy. Typically, inertial response and other auxiliary services are not provided by power. Similarly, fluctuations in power intensify its impact. While fluctuations in energy in smart grid might mitigate load fluctuations, they can magnify frequency aberrations in power networks if they are in antiphase. On the other hand, the likelihood of energy fluctuations, the combination of several frequency fluctuations, and the phase angle between them cannot be determined.

In Table 2 the summary of the typical simulation parameters is indicated. All of the network nodes were randomly assigned to the beacon-enabled mode and ran the simulations. 50 nodes made up the cluster that the gateway generated. There are four distinct radio modes described: broadcasting, receiving, idle, and sleeping. For each state, the time spent is multiplied listening to the radio by the energy use to get the overall consumption. To find out how interference from surrounding devices affected the simulation, clusters from different gateways were run in sequence. On the first second, gateway 1 started working. The second gateway began functioning at 200 s, while the third began at 300 s. Runtime for the simulations was 1000 s. To test how well the proposed scheme worked, NS-2 simulator version 2.34 is used. The algorithms are executed on a 64-bit Windows 10 operating system with an Intel Core i5-5300U CPU and 8 GB of RAM. Installing a hypervisor on a physical server enables VMware server virtualization to operate numerous virtual machines (VMs) on a single physical server. With virtual machines (VMs), it is possible to run numerous operating systems (OSes) on a single physical server. Virtual machines on a single physical server share hardware resources like memory and network bandwidth. The Node configure ration parameters include address type, link layer, interface queue type, physical layer type, medium access control, ad hoc routing protocol, antenna type, propagation types, channel used, mobile IP, energy model, and more.

Table 2. Simulation parameters [22]

Simulation Parameters	
Simulator	Ns-2.34
Protocol	AODV
Simulation Duration	400 sec
Simulation Area	1000m × 1000m
Number of Nodes	50,100
Transmission range	300m
Movement Model	Random Waypoint
Pause Time	50 sec
Packet Rate	4pckts/Sec
Traffic Type	CBR
Data Payload	512 bytes/packet

It is common practice to incorporate randomization into ns-2 implementations; for instance, two TCP Senders competing shall implement both traffic generators that release packets at random times and random sliding-window delays. The random-number generator will always give the same sequence, even though it is feasible to seed it such that various repeats of the same experiment provide different outputs. As a result, running the same ns-2 script should consistently produce the same outcome.

Ratio of successful communications to total communications. If the value is high, it suggests a high level of trust, and if it's low, it indicates harmful actions. Each node calculates a trustworthiness ratio for each of its neighbours using this metric. In this case, the credibility of both the sender and the recipient of a message can be evaluated. When gauging trust directly, a SG node looks at how often messages were sent and received. The neighbours of a SG node are used to determine how trustworthy it is in a recommended trust evaluation. This research considers an EEMLTM-MRS-RRC in Smart Grid that maintains multiple routes by considering the trust factors. The proposed model is compared with the traditional trust-aware multi-objective metaheuristic optimization-based secure clustering with route planning (TAMOMO-SCRP) technique and Trusted Parallel Optimization on Route Planning (T-PORP).

Because the chosen traditional models outperform a large number of other existing models, we compare them to the suggested model. A lot of computing power is usually needed for the complicated algorithms used in trust-aware multi-objective metaheuristic optimization methods. Deployed sensor nodes in smart grids are one example of an environment with restricted processing capabilities and energy constraints that can make it challenging to implement these algorithms. Deployment and real-time operational efficiency in dynamic contexts may be impacted by this extra complexity. Even if trust-aware models try to make things more secure, they might still be vulnerable. Attackers can take advantage of loopholes in the trust evaluation process, compromising the trust models and making hostile nodes seem trustworthy. The routing algorithm's dependability and security are severely jeopardized by this. Further risks may be introduced by managing trust relationships that are dynamic and occurring in real-time.

Models of attacks on smart grids centre on cyber dangers that jeopardize the availability, confidentiality, and integrity of grid operations. These models are useful for figurering out how malware might spread in smart grid settings and finding entry points for attacks. In order to better understand the dynamics of cyber-attacks, researchers have proposed a generic model that encompasses all stages of a cyber attack's lifecycle. Smart grids are vulnerable to a wide variety of threats, such as phishing, data manipulation, and Distributed Denial of Service (DDoS) attacks. Public safety, data integrity, and power supply can all be jeopardized by these attacks. In order to guarantee security, it is necessary to employ comprehensive tactics and customized responses due to the variety of threats.

One way to measure accuracy is by counting how many predictions were right, or by tallying up all of the guesses. All of the models are used to determine the score levels. Improving confidence scores is as simple as following recommended practices when developing models. The time levels represent the total time consumed to complete an operation. The time levels of the proposed model are less and the accuracy levels are high. The calculations are made on the simulation results and the mathematical representations are used to calculate the accuracy levels. Time levels are calculated using the functions that are used to calculate the total time consumed to complete an operation.

Table 3. Node information processing accuracy levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	97.3	94.3	92.4
100	97.6	94.7	92.7
150	97.7	94.9	92.9
200	97.9	95.3	93.1
250	98.0	95.3	93.4
300	98.2	95.6	93.5

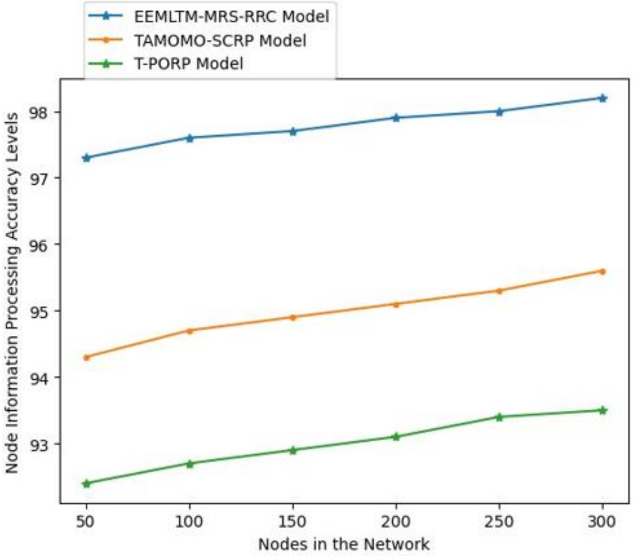

Figure 5. Node information processing accuracy levels

The nodes that need to involve in SG routing model has to update the information with the network authority. The nodes information helps to identify the nodes in the network and to involve in routing and communication. The Node Information Processing Accuracy Levels of the proposed and existing models are shown in Table 3 and Figure 5.

The types of node transactions in the smart grid and their total range are shown in Figure 6. The y axis represents the total samples considered for a particular type and x axis represents the attack type. The types of attacks in the smart grid and the attack ratio are indicated.

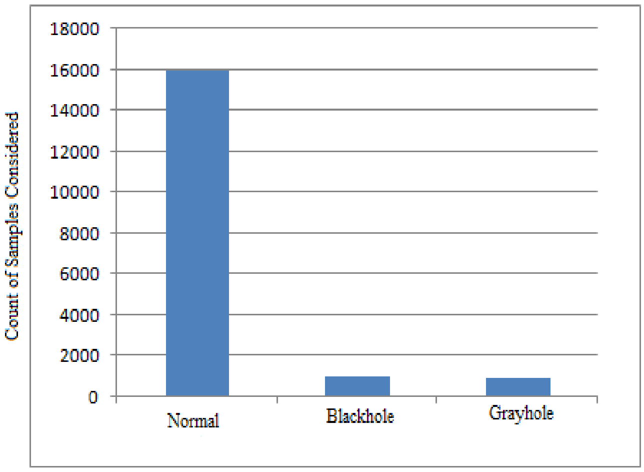

Figure 6. Smart grid attack ratio

Table 4. Node trust factor calculation accuracy levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	97.6	92.8	94.3
100	97.8	93.0	94.5
150	98.0	93.2	94.8
200	98.2	93.5	95.1
250	98.4	93.8	95.4
300	98.5	94	95.6

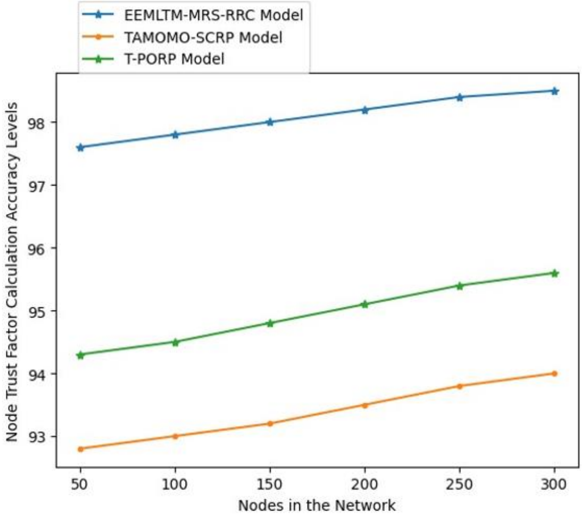

Figure 7. Node trust factor calculation accuracy levels

A node's trust factor is a representation of the node's behavior and attributes. Factors like as packet delivery rate, delay levels, loss levels, and fake data injections are used to determine each node's trust factor. To determine how well a node is doing, we look at its trust factor. The trust factor calculation is done for each node in the network and the trust factor represents the node internal properties. The trust factor represents whether to consider the node or not in routing process. Table 4 and Figure 7 show the Node Trust Factor Calculation Accuracy Levels of the existing and proposed models.

For the purpose of keeping tabs on the network's nodes, the suggested model takes the network's head evaluator node in the SG into account. We will evaluate the NHEN node according to its transmission levels, energy consumption, and performance. The Network Head Evaluator Node Selection Accuracy Levels of the existing and proposed models are depicted in Table 5 and Figure 8.

Table 5. Network head evaluator node selection accuracy levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	97.1	94.1	93.5
100	97.4	94.3	93.7
150	97.7	94.4	93.9
200	97.9	94.7	94.2
250	98.1	94.9	94.4
300	98.4	95.2	94.6

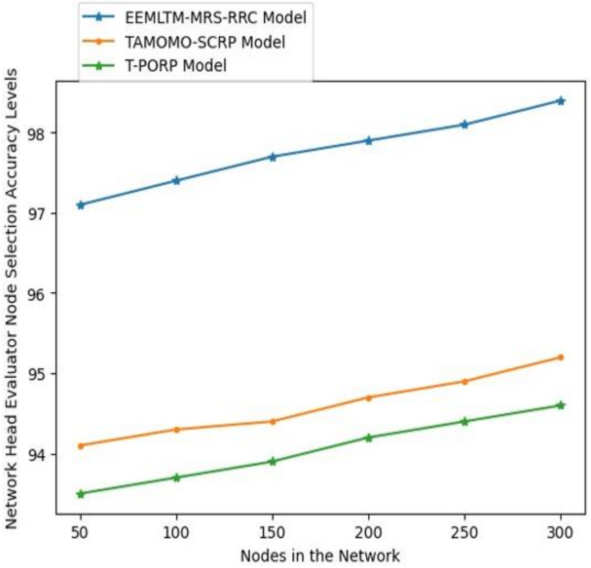

Figure 8. Network head evaluator node selection accuracy levels

Table 6. Node behaviour analysis time levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	14.7	19.9	17.9
100	14.9	20.1	18.1
150	15.1	20.3	18.3
200	15.5	20.6	18.6
250	15.8	20.8	18.9
300	16	21	19

In SG communication, each node consumes its own resources by sending out data packets to its neighbours. In a perfect scenario, all the nodes would send packets to the other nodes based on their individual requirements. The node behaviour analysis is performed by the NHEN node to verify whether there is any data loss or unusual traffic in the network. The Node Behaviour Analysis Time Levels of the existing and proposed models are shown in Table 6 and Figure 9.

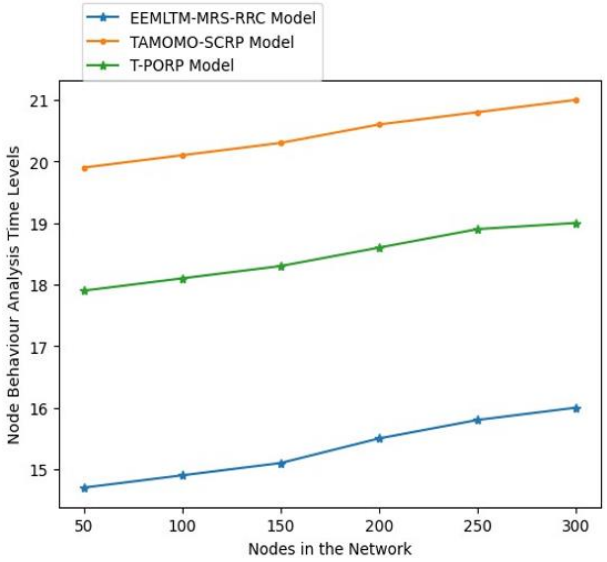

Figure 9. Node Behaviour Analysis Time Levels

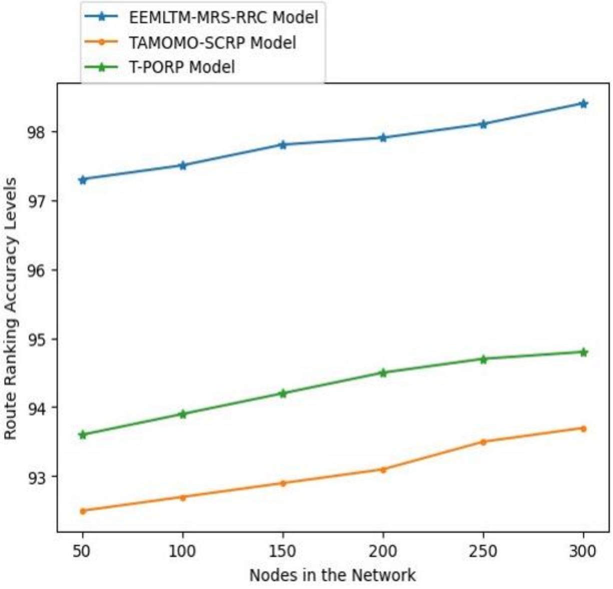

Figure 10. Route ranking accuracy levels

Table 7. Route ranking accuracy levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	97.3	92.5	93.6
100	97.5	92.7	93.9
150	97.8	92.9	94.2
200	97.9	93.1	94.5
250	98.1	93.5	94.7
300	98.4	93.7	94.8

The proposed model performs ranking of the routes identified that are minimum. The ranking is performed to the nodes that are minimum di stance and less energy consumption. The route rankings help in selection of the best ranked routes among the available routes. The Route Ranking Accuracy Levels of the existing and proposed models are depicted in Table 7 and Figure 10.

The correlation factor among the node features is calculated and these features are used for selecting the trusted nodes in the route. The correlation factor of the smart grid node features is shown in Figure 11.

Table 8. Trusted route selection accuracy levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	97.4	94.3	93.5
100	97.6	94.5	93.7
150	97.9	94.7	93.9
200	98.1	94.9	94.1
250	98.4	95.1	94.5
300	98.6	95.4	94.8

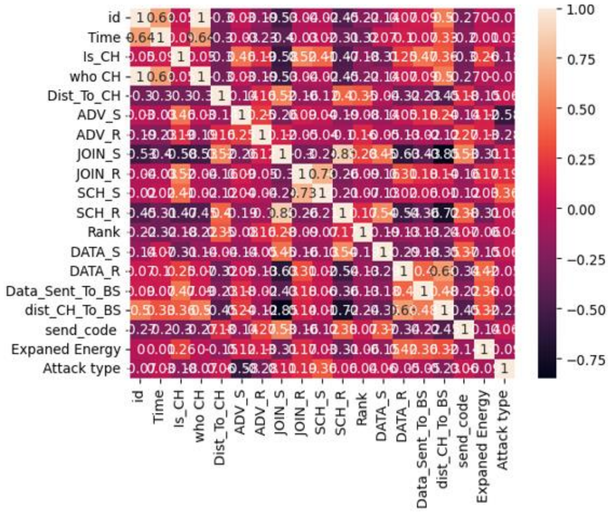

Figure 11. Smart grid nodes correlation factor

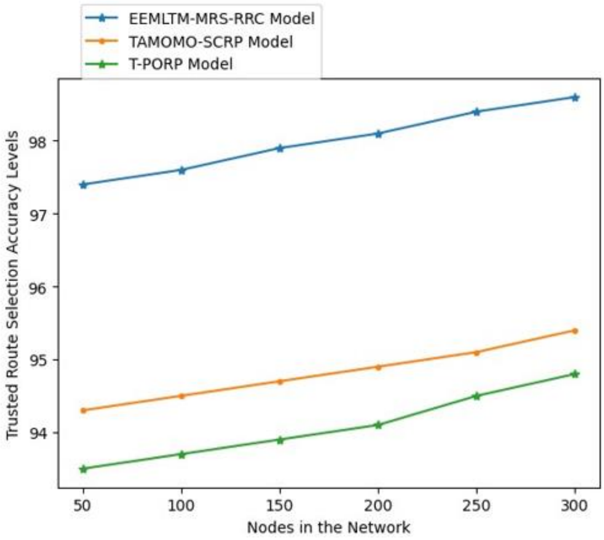

Figure 12. Trusted route selection accuracy levels

The value or metric used by a routing system to measure the distance to a network is what ultimately determines which path it chooses as the optimal one. A metric is a numerical value used to express how far away from a network something is. The shortest path in a network is the optimal one. With the assistance of trusted route selection, the most reliable path can be used to safely transmit data. Table 8 and Figure 12 show the Trusted Route Selection Accuracy Levels of the current and suggested models, respectively.

The proposed model considers the trusted nodes in the network and in routing process. The network contains nodes of normal behaviour avoiding malicious actions in the SG. This helps in reducing the utilization of power in the network. The data is also transmitted in the best shortest path in the SG. The Energy Consumption Reduction Accuracy Levels of the existing and proposed models are depicted in Table 9 and Figure 13.

Table 9. Energy consumption reduction accuracy levels

Nodes in the Network	Models Considered		
	EEMLTM-MRS-RRC Model	TAMOMO-SCRP Model	T-PORP Model
50	97.6	92.9	92.4
100	97.9	93.2	92.7
150	98.1	93.6	92.9
200	98.5	93.9	93.1
250	98.7	94.2	93.4
300	98.8	94.5	93.6

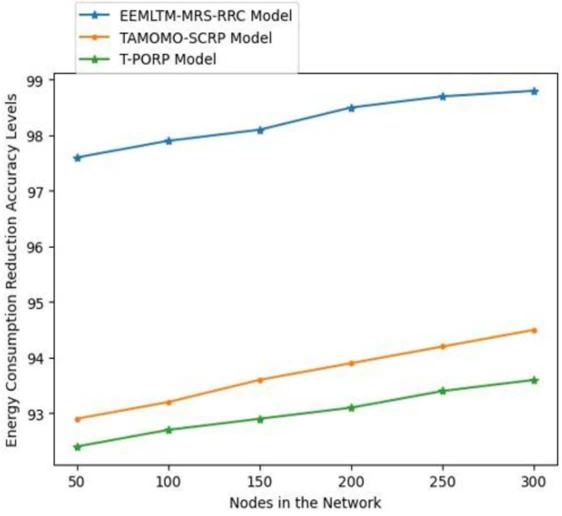

Figure 13. Energy consumption reduction accuracy levels

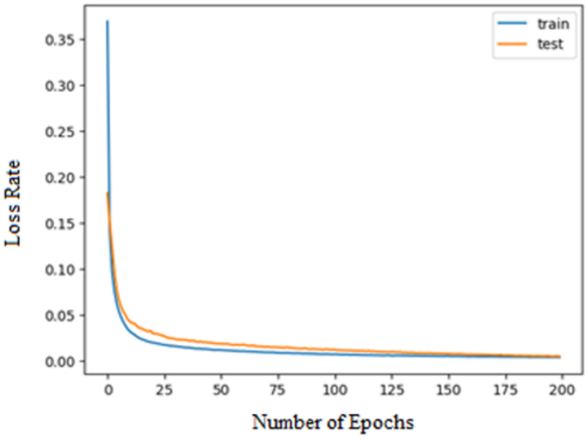

Figure 14. Loss rate

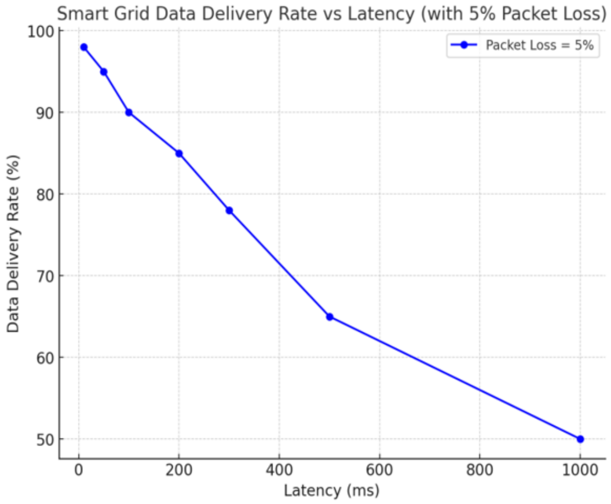

Figure 15. Packet delivery rate Vs latency

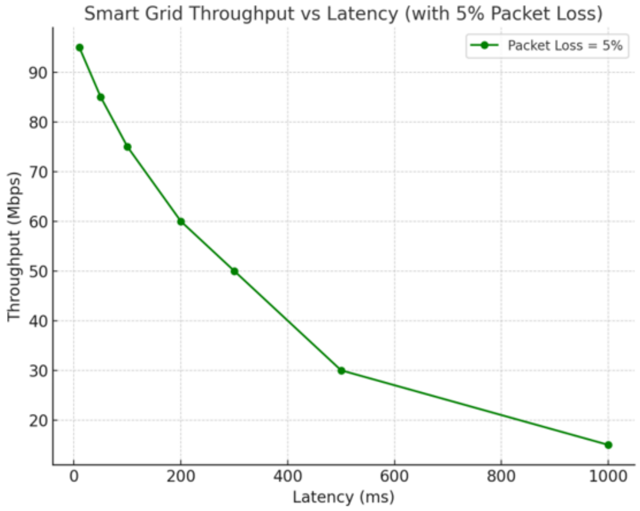

Figure 16. Throughput Vs latency

The loss rate of the model represents the performance levels of the routing model. The less the loss rate, the more the accuracy in route detection will be. The y axis is the loss levels. The loss levels during training and testing phases are indicated in the figure. The proposed model loss rate is shown in Figure 14.

When it comes to smart grid routing performance, the network topology is paramount. The efficiency of data transmission between nodes is affected by the topological structure, which might be tree, mesh, or ring. For example, while tree architectures make data aggregation faster, they can increase latency and introduce potential sites of failure. While mesh topologies improve redundancy and fault tolerance, they can make route administration and calculation more complicated. Another important factor in routing speed is the network's traffic load, or the amount of data that needs to be transmitted at any one time. Longer route recognition times and decreased accuracy might result from strain on routing protocols caused by fluctuations in energy demand, especially during peak hours. The only way to reduce their impact and make sure data packets are properly delivered regardless of the load is to use congestion management measures and load balancing techniques.

Variations in energy production and consumption patterns can be caused by environmental conditions, such as the implementation of renewable energy sources. To accommodate these modifications and the resulting unpredictability of energy flows, dynamic routing adjustments are required. How well routing algorithms respond to these changes depends on how fast they can adjust. The stability of the system depends on routing protocols that can withstand unexpected shifts in generation and demand, according to the studies.

The latency and data delivery rate of the smart grid under various conditions are shown in Figure 15.

The throughput levels Vs latency in the msartgrid is shown in Figure 16.

Despite the transmission time required by the proposed scheme, the delay is within an acceptable range and the research aims to deliver an excellent packet delivery ratio to ensure high smart grid reliability. In addition, we guarantee that the suggested technique achieves top-notch performance. Results from simulations show that the suggested route selection method can reliably transmit data in a smart grid setting.

4. CONCLUSION

The efficiency and dependability of the power grid depend on the power communication network. In both the monitoring-industry and intelligent power grid communication networks, you'll find dispersed nodes in various, complicated locations. By dissecting the smart grid's routing mechanism, we can extend the life of the network and make it more capable. Trust management poses a significant challenge to the IoT and other artificial societies. Since more and more people rely on Internet of Things (IoT) devices and services, the situation has gotten worse. Because of the inherent heterogeneity and volatility of static models, they are no longer useful in the age of big data and IoT devices. An approach to controlling trust in SG devices is suggested in this paper. The suggested approach determines the direct and indirect trust of the SG nodes in the network by utilizing the node's own data. For the purpose of keeping tabs on the whole SG network, this study took into account a network head evaluator node. In order to decrease network latency, a Trust Linked Probabilistic Controller is employed to identify the various shortest paths in the SG. This study proposes a new method of control that takes into account a rank-based cluster model and multi-level trust factors to enhance energy efficiency, reduce fluctuations, and mitigate power quality degradation and power fluctuations caused by the smart grid's integration of large-scale routing models. Minimizing energy swings and making the most efficient use of a storage system for energy are the goals of this technique. Based on theoretical research, the mathematical model of an energy balancing system is employed to conduct a comprehensive analysis of the power fluctuation and smoothing technique. The goal of this approach is to make energy efficiency improvements more precise. In order to keep many routes operational in smart grids, this study examines a multi-level trust model for energy-efficient multi-route selection using rank-based route clusters.The proposed model achieves 98.5% accuracy in trust calculation and 98.4% accuracy in multiple shortest and trusted paths elections for secure data transmissions in SG. In future, optimization techniques can be applied on the multi path routing models for detecting the optimal path and more sensitive parameters of nodes can be considered for trust evaluation and degree of trust-based routing also can be applied for better security levels.

REFERENCES

[1] Nagappan, K., Rajendran, S., Alotaibi, Y. (2022). Trust aware multi-objective metaheuristic optimization based secure route planning technique for cluster based IIOT environment. IEEE Access, 10: 112686-112694. https://doi.org/10.1109/ACCESS.2022.3211971

[2] Li, B., Dai, T., Chen, W., Song, X., Zang, Y.L., Huang, Z.L. (2022). T-PORP: A trusted parallel route planning model on dynamic road networks. IEEE Transactions on Intelligent Transportation Systems, 24(1): 1238-1250. https://doi.org/10.1109/TITS.2022.3216310

[3] Hameed, S., Shah, S.A., Saeed, Q.S., Siddiqui, S., Ali, I., Vedeshin, A., Draheim, D. (2021). A scalable key and trust management solution for IoT sensors using SDN and blockchain technology. IEEE Sensors Journal, 21(6): 8716-8733. https://doi.org/10.1109/JSEN.2021.3052009

[4] Dass, P., Misra, S., Roy, C. (2020). T-safe: Trustworthy service provisioning for IoT-based intelligent transport systems. IEEE Transactions on Vehicular Technology, 69(9): 9509-9517. https://doi.org/10.1109/TVT.2020.3004047

[5] Li, L., Chang, L., Song, F. (2020). A smart collaborative routing protocol for QoE enhancement in multi-hop wireless networks. IEEE Access, 8: 100963-100973. https://doi.org/10.1109/ACCESS.2020.2997350

[6] Ruiz, L., Barroso, R.J.D., De Miguel, I., Merayo, N., Aguado, J.C., Abril, E.J. (2021). Routing, modulation and spectrum assignment algorithm using multi-path routing and best-fit. IEEE Access, 9: 111633-111650. https://doi.org/10.1109/ACCESS.2021.3101998

[7] Goswami, P., Mukherjee, A., Hazra, R., Yang, L., Ghosh, U., Qi, Y., Wang, H. (2021). AI based energy efficient routing protocol for intelligent transportation system. IEEE Transactions on Intelligent Transportation Systems, 23(2): 1670-1679. https://doi.org/10.1109/TITS.2021.3107527

[8] Mo, W., Liu, W., Huang, G., Xiong, N.N., Liu, A., Zhang, S. (2021). A cloud-assisted reliable trust computing scheme for data collection in internet of things. IEEE Transactions on Industrial Informatics, 18(7): 4969-4980. https://doi.org/10.1109/TII.2021.3108149

[9] Velusamy, D., Pugalendhi, G. (2020). Water cycle algorithm tuned fuzzy expert system for trusted routing in smart grid communication network. IEEE Transactions on Fuzzy Systems, 28(6): 1167-1177. https://doi.org/10.1109/TFUZZ.2020.2968833

[10] Wang, X., Zhang, P., Du, Y., Qi, M. (2020). Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network. IEEE Access, 8: 47675-47693. https://doi.org/10.1109/ACCESS.2020.2978143

[11] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., Wu, D. O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials, 22(4): 2462-2488. https://doi.org/10.1109/COMST.2020.3009103

[12] Yang, H., Bao, B., Li, C., Yao, Q., Yu, A., Zhang, J., Ji, Y. (2021). Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial IoT. IEEE Internet of Things Journal, 9(3): 2419-2431. https://doi.org/10.1109/JIOT.2021.3097440

[13] Krishnan, P., Jain, K., Achuthan, K., Buyya, R. (2021). Software-defined security-by-contract for blockchain-enabled MUD-aware industrial IoT edge networks. IEEE Transactions on Industrial Informatics, 18(10): 7068-7076. https://doi.org/10.1109/TII.2021.3084341

[14] Sadrishojaei, M., Jafari Navimipour, N., Reshadi, M., Hosseinzadeh, M., Unal, M. (2022). An energy-aware clustering method in the IoT using a swarm-based algorithm. Wireless Networks, 28(1): 125-136. https://doi.org/10.1007/s11276-021-02804-x

[15] Musil, P., Mlynek, P., Slacik, J., Pokorny, J. (2020). Simulation-based evaluation of the performance of broadband over power lines with multiple repeaters in linear topology of distribution substations. Applied Sciences, 10(19): 6879. https://doi.org/10.3390/app10196879

[16] Wang, J., Lim, M.K., Wang, C., Tseng, M.L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. Computers & Industrial Engineering, 155: 107174. https://doi.org/10.1016/j.cie.2021.107174

[17] Liu, L., Wang, Y., Meng, W., Xu, Z., Gao, W., Ma, Z. (2021). Towards efficient and energy-aware query processing for industrial internet of things. Peer-to-Peer Networking and Applications, 14(6): 3895-3914. https://doi.org/10.1007/s12083-021-01163-w

[18] Cao, J., Wang, X., Huang, M., Yi, B., He, Q. (2021). A security-driven network architecture for routing in industrial Internet of Things. Transactions on Emerging Telecommunications Technologies, 32(4): e4216. https://doi.org/10.1002/ett.4216

[19] Raza, N., Akbar, M.Q., Soofi, A.A., Akbar, S. (2019). Study of smart grid communication network architectures and technologies. Journal of Computer and Communications, 7(3): 19-29. https://doi.org/10.4236/jcc.2019.73003

[20] Sutagundar, A.V., Manvi, S.S., Balavalad, K.B. (2010). Energy efficient multipath routing protocol for WMSNs. International Journal of Computer and Electrical Engineering, 2(3): 503-510.

[21] Pokhrel, S.R., Verma, S., Garg, S., Sharma, A.K., Choi, J. (2020). An efficient clustering framework for massive sensor networking in industrial Internet of Things. IEEE Transactions on Industrial Informatics, 17(7): 4917-4924. https://doi.org/10.1109/TII.2020.3006276

[22] Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K.H., Pathan, M.S., Hussain, M.I., Memon, M.Q. (2019). A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. Future Internet, 11(3): 61. https://doi.org/10.3390/fi11030061

[23] Zhang, W., Wang, X., Han, G., Peng, Y., Guizani, M. (2021). SFPAG-R: A reliable routing algorithm based on sealed first-price auction games for industrial Internet of Things networks. IEEE Transactions on Vehicular Technology, 70(5): 5016-5027. https://doi.org/10.1109/TVT.2021.3074398

[24] Cao, J., Wang, X., Huang, M., Zhou, X. (2019). A mobility-supported routing mechanism in industrial IoT networks. IEEE Access, 7: 25603-25615. https://doi.org/10.1109/ACCESS.2019.2900289

[25] Al-Zubaidie, M., Zhang, Z., Zhang, J. (2020). REISCH:

Incorporating lightweight and reliable algorithms into healthcare applications of WSNs. Applied Sciences, 10(6): 2007. https://doi.org/10.3390/app10062007

[26] Lakshmanna, K., Subramani, N., Alotaibi, Y., Alghamdi, S., Khalafand, O.I., Nanda, A.K. (2022). Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks. Sustainability, 14(13): 7712. https://doi.org/10.3390/su14137712

[27] Nicaire, N.F., Steve, P.N., Salome, N.E., Grégroire, A.O. (2021). Parameter estimation of the photovoltaic system using bald eagle search (BES) algorithm. International Journal of Photoenergy, 2021(1): 4343203. https://doi.org/10.1155/2021/4343203

[28] Jagannathan, P., Gurumoorthy, S., Stateczny, A., Divakarachar, P.B., Sengupta, J. (2021). Collision-aware routing using multi-objective seagull optimization algorithm for WSN-based IoT. Sensors, 21(24): 8496. https://doi.org/10.3390/s21248496

[29] Tamilvizhi, T., Surendran, R., Krishnaraj, N. (2021). Cloud based smart vehicle tracking system. In 2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, pp. 1-6. https://doi.org/10.1109/iCCECE52344.2021.9534843

[30] Tamilvizhi, T., Surendran, R., Romero, C.A. T., Sendil, M.S. (2022). Privacy preserving reliable data transmission in cluster based vehicular adhoc networks. Intelligent Automation & Soft Computing, 34(2): 1265-1279. https://doi.org/10.32604/iasc.2022.026331

[31] Tamilvizhi, T., Surendran, R., Anbazhagan, K., Rajkumar, K. (2022). Quantum behaved particle swarm optimization-based deep transfer learning model for sugarcane leaf disease detection and classification. Mathematical Problems in Engineering, 2022(1): 3452413. https://doi.org/10.1155/2022/3452413

[32] Riya, K.S., Surendran, R., Tavera Romero, C.A., Sendil, M.S. (2023). Encryption with user authentication model for internet of medical things environment. Intelligent Automation & Soft Computing, 35(1): 507-520. https://doi.org/10.32604/iasc.2023.027779

[33] Krishnaraj, N., Sangeetha, S. (2022). A study of data privacy in Internet of Things using privacy preserving techniques with its management. International Journal of Engineering Trends and Technology, 70(2): 43-52.

[34] Alsattar, H.A., Zaidan, A.A., Zaidan, B.B. (2020). Novel meta-heuristic bald eagle search optimisation algorithm. Artificial Intelligence Review, 53: 2237-2264. https://doi.org/10.1007/s10462-019-09732-5

[35] Goswami, P., Mukherjee, A., Maiti, M., Tyagi, S.K.S., Yang, L. (2021). A neural-network-based optimal resource allocation method for secure IIoT network. IEEE Internet of Things Journal, 9(4): 2538-2544. https://doi.org/10.1109/JIOT.2021.3084636

[36] Li, X., Zhu, L., Chu, X., Fu, H. (2020). Edge computing-enabled wireless sensor networks for multiple data collection tasks in smart agriculture. Journal of Sensors, 2020(1): 4398061. https://doi.org/10.1155/2020/4398061