Vol.67: e24240207, 2024
https://doi.org/10.1590/1678-4324-2024240207
ISSN 1678-4324 Online Edition

BABT
Brazilian Archives of Biology and Technology

Article - Engineering, Technology and Techniques

Enhancing Trust Management Using Locally Weighted Salp Swarm Algorithm with Deep learning for SIoT Networks

Murugesan Gurusamy[1]
https://orcid.org/0009-0005-9084-2109

Maheswara Venkatesh Panchavarnam[2*]
https://orcid.org/0009-0003-2511-9040

Jayasankar Thangaiyan[2]
https://orcid.org/0000-0001-7398-343X

[1]Anjalai Ammal Mahalingam Engineering College, Dept. of ECE, Thiruvarur Tamil Nadu, India; [2]University College of Engineering,Dept. of ECE, Anna University, Tiruchirappalli, Tamil Nadu, India.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Fabio Alessandro Guerra

Received: 02-May-2024; Accepted: 13-May-2024.

*Correspondence: maheshwaravenkatesh@gmail.com (M.P).

HIGHLIGHTS

- ETM-LWSSADL algorithm achieves a better solution with the highest possible RESE values.
- BiGRU model is applied to generate a THV on collected traffic data.
- ETM-LWSSADL technique exploits the LWSSA technique for optimum hyperparameter selection.

Abstract: The Trust-Aware Aggregation Authentication Protocol for SIoT Networks is a security process intended for SIoT platforms. It concentrates on ensuring the reliability of communication and data aggregation between interrelated IoT devices. This protocol deploys authentication systems for verifying the identities of devices and integrates trust-aware mechanisms to estimate the trustworthiness of data exchanged from the social environment of SIoT. By establishing a trustworthy and secure communication structure, this protocol improves the entire integrity and security of SIoT networks, addressing potential vulnerabilities connected with social communications between IoT devices. Therefore, this study develops an enhanced Trust Management using Locally Weighted Salp Swarm Algorithm with Deep learning (ETM-LWSSADL) technique for SIoT Networks. The ETM-LWSSADL technique computes direct and indirect trust values and is assessed depending upon different weighing factors for maximizing the application performance and creating a secure data transmission process. During authentication process, when the SIoT device with total trust value (TTV)is not greater than the threshold value (THV) or authentication token is invalid, the gateways then disregard the node. Besides, bidirectional gated recurrent unit (BiGRU) model is applied to generate a THV on collected traffic data. Moreover, the ETM-LWSSADL technique exploits the LWSSA technique for optimum hyper parameter selection of the BiGRU algorithm. To highlight the enhanced performance of the ETM-LWSSADL methodology, an extensive range of simulations can be involved.

Keywords: Social Internet of Things, Trust and Reputation Management, Salp Swarm Algorithm, Deep Learning, Threshold Value.

INTRODUCTION

The Internet of Things (IoT) includes of huge number of devices with capability to detect, collect, and generate data all over the world [1]. The devices communicate with each other to provide an extensive of smart services that will be employed by users, manufacturers, and alternative devices to perform day-to-day activities. IoTs have applicability in several fields such as medical field, intelligent transportation systems (ITS), workstations and smart homes, environment monitoring, and more [2]. Every device in IoT performs the role of service requestor, service provider, or both. In order to develop trusted correlation between devices, social networking platform was employed in IoT and this model was named SIoT. SIoT includes different things or devices to collect the data, provide services, create verdicts, offer recommendations, and take action [3]. It has a vital effect on restoring the innovative developments of medical-embedded sensors, medical robotics, and medical facilities. SIoTis also employed for coastal management systems, and crowd-sensing applications [4]. With the help of SIoT, the social networking of device owners has been utilized to establish a trustworthy social correlation between the devices.

In order to ensure trustworthy cooperation among individuals, soft security utilizes social control facets to the basic security method [5]. For instance, soft trust could be dependent upon direct involvement (direct trust), trustworthy peer involvement gathered in the period (indirect trust), or both [6]. A trust engine named the Trust and Reputation Management (TRM) model obviously calculates the trust level. The TRM model collects data from the individuals that the service is about the quality of service (QoS) obtained and calculates the statuses of the individuals that are offered the service. In a distributive TRM model, the service consumer will be learned the previous behaviour of service provider via straight collaborations [7]. However, once the service provider does not have satisfactory direct communications with the particular service user, it should be reliant on an indirect experience calculated from the recommendations acquired from peers who can be previously directly communicated with the service provider [8]. Reputation could be calculated depending on indirect trust, direct trust, or both. The TRM model should be organized to manage adaptable settings and malicious individuals. The major significant need of the TRM model was adaptively maintenance. The help of TRM to overcome the adaptive condition permits trusters to find the modifications in recommender behaviour or service providers [9]. In IoT, individuals become heterogeneous and measure several self-interest populations and the probability of consistent reports will be difficult. In order to adversely impact the artificial increase of the reputation of a bad service provider (ballot-stuffing) and the better service provider reputation (bad-mouthing), recommenders may be provided incorrect recommendations [10].

This study develops an enhanced Trust Management using Locally Weighted Salp Swarm Algorithm with Deep learning (ETM-LWSSADL) technique for SIoT Networks. During authentication process, when the SIoT device with total trust value (TTV) is not greater than the threshold value (THV) or authentication token is invalid, the gateways then disregard the node. Besides, bi-directional gated recurrent unit (BiGRU) model has been applied to generate a THV on collected traffic data. Moreover, the ETM-LWSSADL technique exploits the LWSSA technique for optimal hyperparameter selection of the BiGRU model. The experimental outcomes highlighted that the ETM-LWSSADL technique gains maximum performance over other models.

RELATED WORKS

Cheng and coauthors [11] developed a lightweight authentication-driven trusted management model, which comprises an innovative authentication and key contract method for assurance of the validity of task issuers, with significantly decreased expenses than other studies. The method also integrates a dispersed information storage system and fine-grained access control method. This technique records the interactive messages under the blockchain (BC) to confirm traceability. In [12], an innovative dynamic and scalable multi-level Trust-Model (DSL-STM) system was developed, particularly developed for SIoT platforms. The technique also developed multidimensional metrics to define a SIoT individual's behaviours. Combination through an ML-based algorithm. Lastly, a hybrid propagation technique was developed to distribute trusted values at the network, reducing resource consumption and protective scalability and dynamism. Roy and coauthors [13] introduced an autonomous decentralized trust management system to choose a trustworthy device for demanded service transactions. This presented method employs the Social IoTs for trust management. The developed method utilizes social relationships to determine the level of trust between relevant devices, evaluate the overall trust of the unknown devices, periodically upgrade the experimental trust parameters, and separate the malicious nodes across the network.

In [14], a Social Internet of Vehicles—Fuzzy-based Trustworthy Friendship Selection Algorithm—Crossover-boosted AOA (SIoV-FTFSA-CAOA) technique was introduced. This technique employs FL. The Crossover-boosted Arithmetic Optimizer method was employed for recognizing the communities. The maximum trust value selection method was also deployed. The Road Aware Geographical Routing protocol has been employed, and Battery Model-based Energy Computation technique was employed. Wang and coauthors [15] developed a BC-empowered model involving 3 components for accomplishing decentralized TM in IoBT: (i) Local Trust Computation: every IoBT node employs a local trust computation technique; (ii) Global Trust Aggregation: portable ping-pong positions utilize a global trust combination method; (iii) BC Consensus Process: the global trusts of IoBT nodes have been upgraded to the BC. The technique established an innovative consensus method that activates BC nodes.

In [16], an innovative behavioural profiling system was introduced that employs AI methods. Simulated data was formed to reproduce different conditions, including discrepancies in security protocols, device qualities, environmental effects, network settings, and application workloads. The effectiveness of the proposed solution was evaluated by performing 6 simulated sequences, where the consequences indicate different values of accuracy in employing multi-factor authentication (MFA). Sharma and coauthors [17] introduced a direct observation-based distributed trust management system, named BD-Trust. During this, BD-Trust reckons under three trust factors. Data trust will be calculated and reliability in established data values for effective communication responses. BD-Trust utilizes a trust update method. An adaptive decay parameter was developed for considering earlier experiential trust values in existing computation while upgrading the trust scores.

Motivation

The Trust-Aware Aggregation Authentication Protocol for Social Internet of Things (SIoT) networks was developed in response to the increasing number of social networks that are being linked with the IoT. As more and more physical objects join the network and communicate data about their social environments, it is crucial to guarantee the reliability and security of data aggregation and communication amongst these devices. This is due to the fact that information gathered via social media is becoming increasingly commonplace. When it comes to the IoT, conventional security measures may fall short when faced with the unique challenges posed by people's interactions and connections. To get around these problems, the Trust-Aware Aggregation Authentication Protocol focuses on trust management and authentication processes tailored to IoT devices. The protocol enhances the general security and integrity of SIoT networks by establishing a secure framework for communication. To do this, we verify the devices' identities and use trust-aware algorithms to determine how reliable the transmitted data is in a social setting.

To counter this, the study recommends an enhanced Trust Management method called ETM-LWSSADL, which combines a Locally Weighted Salp Swarm Algorithm with Deep Learning, to strengthen the safety and efficiency of SIoT networks. This approach calculates direct and indirect trust values by considering a multitude of weighting criteria, all with the goal of optimising the application's performance and ensuring the data transfer's safety. During authentication, the protocol does not pay attention to nodes that do not have sufficient trust or that use incorrect tokens. The SIoT devices' total trust value (TTV) is compared to a threshold value (THV) to achieve this. In addition, the trust handling value (THV) may be improved by the use of a bidirectional gated recurrent unit (BiGRU) model, which is trained using traffic data.

ETM-LWSSADL method utilises the Locally Weighted Salp Swarm Algorithm to determine the optimal BiGRU algorithm hyper parameters, hence enhancing the machine learning algorithm's performance even further. Validating the effectiveness of the ETM-LWSSADL technique may be achieved through thorough simulations. By running these simulations, we can see that the ETM-LWSSADL approach outperformed the competition. The experimental findings reveal that the proposed strategy improves security, reliability, and performance when applied to SIoT networks, suggesting that it might be useful in the real world.

THE PROPOSED METHOD

In this study, we have established an ETM-LWSSADL technique for SIoT Networks. In the presented ETM-LWSSADL technique, the TTV of every SIoT device is derived by the use of behaviour trust and data trust. During authentication process, when the SIoT device with TTV is not greater than THV or authentication token is invalid, the gateways then disregard the node. The BiGRU model on gathered traffic data dynamically determines the THV. Finally, the LWSSA technique can be utilized for optimal hyperparameter selection. Figure 1 represents the entire flow of ETM-LWSSADL technique.

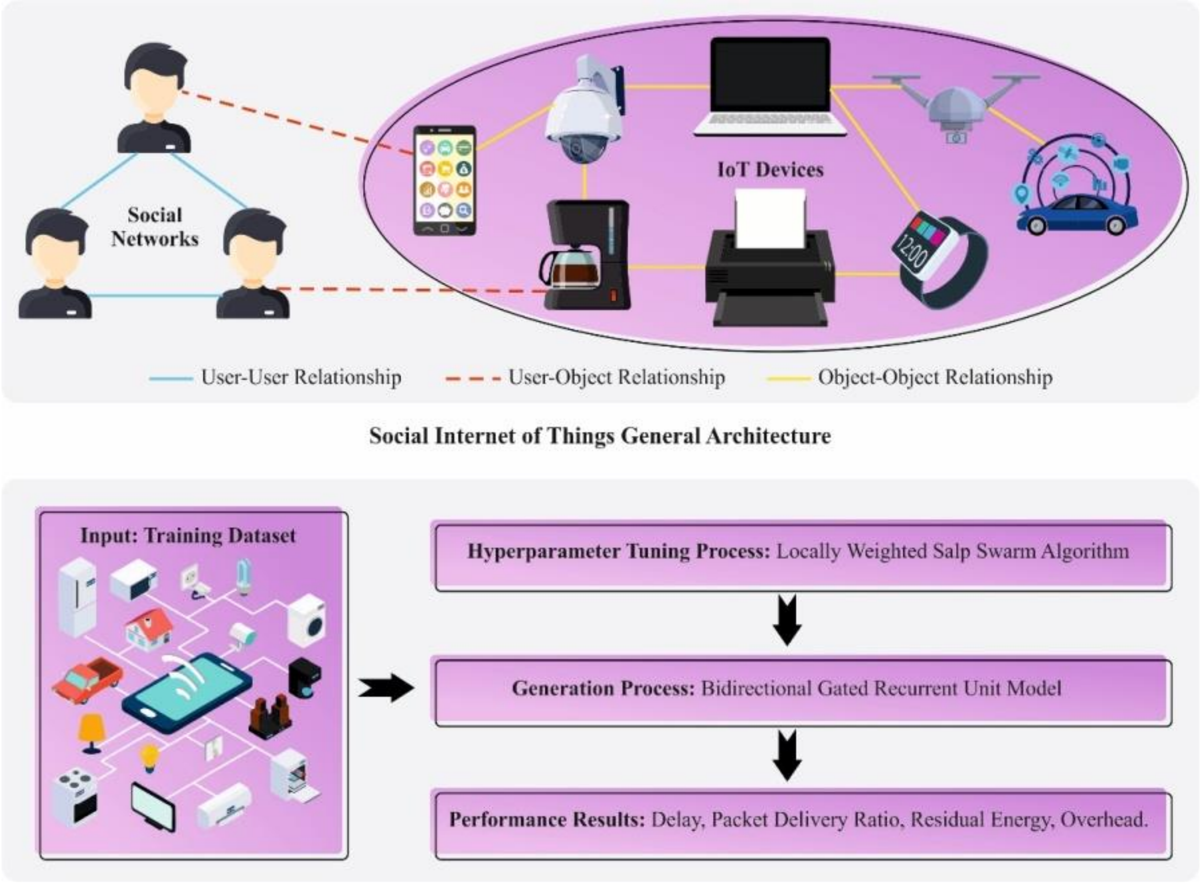
Social
Networks
IoT Devices
User-User Relationship
User-Object Relationship
Object-Object Relationship
Social Internet of Things General Architecture
Input: Training Dataset
Hyperparameter Tuning Process: Locally Weighted Salp Swarm Algorithm
Generation Process: Bidirectional Gated Recurrent Unit Model
Performance Results: Delay, Packet Delivery Ratio, Residual Energy, Overhead.

Figure 1. Overall flow of ETM-LWSSADL technique

Computation of Trust

To enhance reliability amongst SIoT nodes, two kinds of trusts can be measured such as Direct or Indirect trusts [18]. Once nodes i and $j$relate directly with every other the trust can be evaluated as:

$$T_{ij}^{X}(t)=\alpha T_{ij}^{X}(t)(t\text{-}\Delta t)+\alpha D_{ij}^{X}(t)+\beta G_{ij}^{X}+\alpha\beta DP_{ij}^{X} \quad (1)$$

Whereas $X=$ honesty, cooperativeness, community interest, and energy. $T_{ij}^{X}(t)$ implies the past trust among$i$ and $j$interms of X. Δtdenotes the time passedthen the final trust upgrade. Node i will utilize direct trust$D_{ij}^{X}(t)$ and its past trust $T_{ij}^{X}(t)(t-\Delta t)$nearby node j. Besides, these 2 parameters node i also utilizes the centrality and dependability factors to calculate trust. The node centrality was calculated based on Eq. (2).

Centrality G_{ij}^{X}= set of common friends between i and j/Neighbors between i, j (2)

The dependability factor is in the interval of zero and one that is attained by the utilities of another relatedtoSIoTplatform. The behavior of similar node (past history) in a distinct platform can be employed for measuring the reliability. Nodes are recognized by their semantics. The expense linked with collecting the reliability factor is minimal, and in some instances, the reliability factor maybe 0 if similar objects cannot interact with the outside world at all. Once node $i$witnesses node $k$that has already expert transaction with node j, afterward trust can be calculated based on Eq. (3). Node i utilizes k's recommendation to judge node j. Node $i$could not have some direct communication with node $j$in its place utilize recommendation of $k$nearby$jR_{kj}^{X}(t)$ and the past trust value $T_{ij}^{X}(t)(t-\Delta t)$ to allow$j$.According to this, the dependabilityand centrality factorsallowoptimum computation of trust.

$$T_{ij}^{X}(t)=\gamma T_{ij}^{X}(t)(t\text{-}\Delta t)+\gamma D_{ik}^{X}(t)+\gamma R_{kj}^{X}(t)+\beta G_{ij}^{X} \quad (3)$$

$T_{ij}^{X}(t)(t-\Delta r)$denotes the past trust value, $R_{kj}^{X}(t)$signifies the recommendation that node $k$offers to node $i$on node j. There are potential probabilitiesof node k being malicious. If node k is not malicious $R_{kj}^{X}(t)$equivalentsD_{ik}^{X}. If node k is malicious it executesbad-mouthing threats and transmits themsimilar to node i. To prevent that, node i utilizes direct trust to access node $kD_{ik}^{X}(t)$. Composed with these parameters, the trust has been evaluated utilizing centrality and dependability factorsexpressed in Eqs. (2) and (3).

BiGRU based Threshold Value Selection

In this work, the BiGRU model is applied to generate a THV on collected traffic data. The bidirectional RNN can be employed in forward and reverse data [19]. In this study, the NN architecture designed by Grüßer-Sinopoli and Thalemannis to be used, with the standard RNN cells being changed with GRU cells. The BiGRU has connected two hidden layers (HL) in opposed transmitting manner to the similar output layer thus, it achieves data at the past and future conditions. The BiGRU-NN can be the ability to learn the data from 2 various data directions, to create more precise predictions. The concept of the BiGRU is to divide the consistent GRU neurons into backward positions (negative time direction) and forward positions (positive time direction).

Now, the GRU cell has two gates like reset gate (r_t) and update gate (z_t). The update gate z_t controls the quantification of new data from input data arrives the existing condition; the huge z_t, the increasingly additional data can be accessible from the input data. The reset gate (r_t)measures the range to which status data in earlier times will be unnoticed; the small the r_t, the data of the prior state will be disregarded. At time $t,\ x_t$ signifies the input and h_t denote the hidden state. The representation $\otimes$ denotes the element-wise multiplication. $\tilde{h}_t$, also named as the candidate vector, is a modulate function that determines the level to which the new input data will be obtained in the cell status. σ refers to the sigmoid function, and $tanh$ characterizes the $\tanh$ function. The upgrade gate (z) and the reset gate (r) have been computed as presented in Eqs. (4)-(8), where W_r, W_Z and $W_{\tilde{h}_t}$ describes the weight matrices. [] point to that the two vectors will be connected, and the symbol $*$ signifies the element-wise multiplication. Figure 2 illustrates the infrastructure of BiGRU.

$$r_t=\sigma(W_r\cdot[h_{t-1}, x_t]) \tag{4}$$

$$z_t=\sigma(W_Z\cdot[h_{t-1}, x_t]) \tag{5}$$

$$\tilde{h}_t=\tanh\left(W_{\tilde{h}_t}\cdot[r_t*h_{t-1}, x_t]\right) \tag{6}$$

$$h_t=(1-z_t)*h_{t-1}+z_t*\tilde{h}_t \tag{7}$$

$$y_t=\sigma(W_o\cdot t) \tag{8}$$

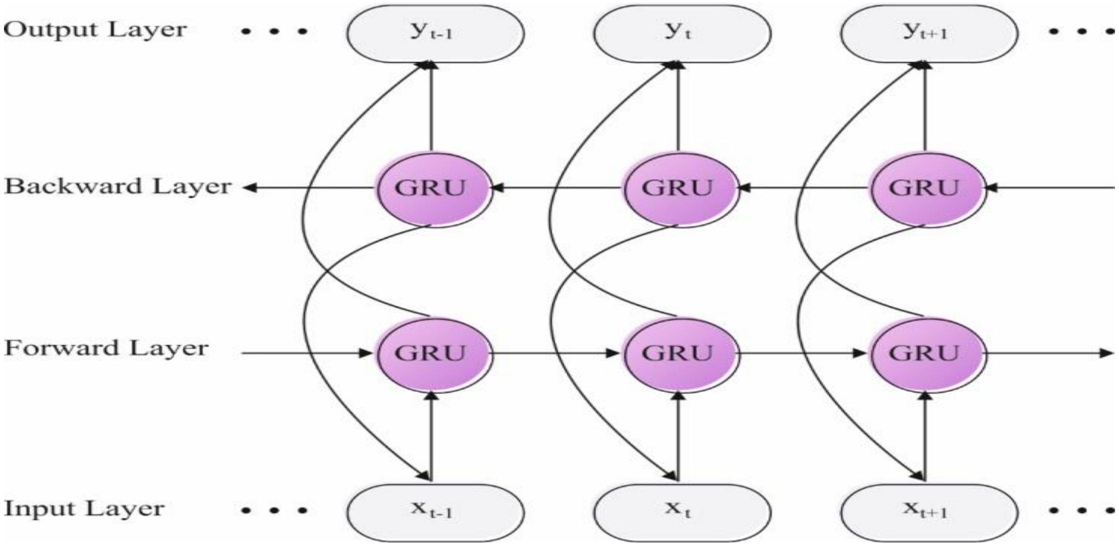

Figure 2. BiGRU architecture

Hyperparameter Tuning using LWSSA

The ETM-LWSSADL technique exploits the LWSSA technique for optimal parameter choice of the BiGRU model. SSA is a biologically inspired optimization manner based on the group behaviors of Salp, ocean invertebrates well-known for swarming patterns [20]. SSA is intended to address the optimizer problems by imitating the cooperation observed and social interaction in Salp swarm. The mathematical formulation is used to govern the decision making process and movement of virtual Salps within the search range. The SSA includes the upgrade of Salp's location in the problem space based on the collective effect of entire swarm, its existing location, and the influence of obtained optimum solution. The position updating formula is given below:

$$y_{1,j}^{t+1}=\begin{cases}F_j+w_1\left(\left(ub_j-lb_j\right)w_2+lb_j\right);\ w_3\geq0.5\\F_j-w_1\left(\left(ub_j-lb_j\right)w_2+lb_j\right);\ w_3<0.5\end{cases} \tag{9}$$

$y_{1,j}^{t+1}$ and F_j are the coordinates of primary Salp location and the position of food supply at j^{Th} dimension, correspondingly. ub_j and lb_j are the upper and lower boundaries of the search space. The two scales w_2 and w_3 are random integer within$[0,1]$. w_1 is a parameter which achieves constancy during exploration and exploitation, it also represents a critical point parameter.

$$w_1=2e^{\left(\frac{-4t}{T}\right)^2} \tag{10}$$

T denotes the maximal iteration count, and the existing iteration is t. Eq. (11) is used to define the update location in relation to the follower salp:

$$y_{i,j}^{t+1}=\frac{1}{2}\left(y_{i,j}^{t}+y_{i-1,j}^{t}\right) \tag{11}$$

$y_{i-1,j}^{t}$ indicates the location of $i-1$ followers at j^{th} dimension. Eq. (11) relies on Eq. (12) (Newton's law of motion):

$$y_{i,j}^{t}=\frac{1}{2}a\times time^2+u_0\times time \tag{12}$$

$y_{i,j}^{t}$ indicates the i^{th}followers location at j^{th}dimension, $time$ represents the time per iteration, u_0 shows the initial speed:

$$a=\frac{u_{final}}{u_0} \tag{13}$$

In Eq. (13), u_0 and u_0 are the initial and the final speed. Eqs. (9) and (11) used to update the leader and follower position. Followers mimic the leader's action still the maximal iteration is attained, while the leader itself can be upgraded according to the food source availability. In the iteration process, the exploration stage of the algorithm makes room for the exploitation stage, which is marked by the downward trend in the w_1 parameter. It can be necessary to have a balance among global as well as local search processes to avoid local optima and rather search for the best global optima.

The local search (locally weighted (LW) algorithm) is a heuristic approach to searching for the solution to the optimization problems. It seamlessly changes the existing solution with the adjacent result within the search range. The amount of possible neighbors for the solution is infinite, hence the key to an effective LW algorithm is to find an efficient method for selecting the suitable neighbor. After each iteration, the LW approach is used to develop the Salp or existing solution.

Firstly, at iteration t, a population pop^t with size of $Npop$salp and a solution $y_i^t=\left(y_{i,1}^t,y_{i,2}^t,\dots y_{i,dim}^t\right)$ is enhanced by the SSA and becomes$xnew_i^t$, then, this salp was enhanced by the LW to become $ynew_i^t$ based on Eq. (14):

$$weight_j=\frac{1}{\left(1+\exp\left(xnew_i^t-y_{i,j}^t\right)\right)} \tag{14}$$

$$ynew_i^t=xnew_{ii}^t+Z\times\left(weight_j\times\left(y_{r_1,j}^t-y_{r_2,j}^t\right)\right) \tag{15}$$

Where $i=l,2,\dots Npop$, $y_{r_1,j}^t,y_{r_2,j}^t$ are randomly chosen two particles from the population pop^t (except the existing particley_i^t). Also, Z represents random number produced by the magenta algorithm according to Levy distribution:

$$z=0.01\times\frac{b}{|q|^{\frac{1}{\propto}}} \tag{16}$$

In Eq. (16), b and q are uniformly distributed as $b\sim N(0,\beta^2)$ and $q\sim N(0,\beta^2)$:

$$\beta=\sqrt[\alpha]{\frac{\Gamma(1+\infty)\sin\left(\frac{\pi\alpha}{2}\right)}{\Gamma\left\lceil\frac{\alpha+1}{2}\right\rceil\alpha 2^{\frac{\alpha-1}{2}}}} \tag{17}$$

In Eq. (17), α indicates the index of stability$\alpha\epsilon[0,2]$.

The fitness choice is a major aspect controlling the efficiency of LWSSA. The parameter choice procedure contains encoded results to measure the performance of the candidate results. During this case, the LWSSA assumes that the accuracy as main condition to plan the FF that is written as:

$$\text{Fitness} = \max\ (P) \tag{18}$$

$$P=\frac{TP}{TP+FP} \tag{19}$$

Whereas, $TP$and FP demonstrate the true and false positive rates

EXPERIMENTAL VALIDATION

In this section, performance analysis of the ETM-LWSSADL algorithm is clearly studied.

In Table 1, the comparison study of the ETM-LWSSADL technique is studied in terms of delay (DEL) and packet delivery ratio (PDR) [21].

Figure 3 represents a comparative DEL result of the ETM-LWSSADL technique under varying monitoring intervals (MIs). The figure indicate that the TMM model reaches worse performance with increased DEL values whereas the TAAPML model attain slightly decreased DEL values. However, the ETM-LWSSADL technique reaches better performance with least DEL values of 35.31ms, 36.16ms, 36.49ms, 36.62ms, and 37.10ms, correspondingly.

Table 1. DEL and PDR analysis of ETM-LWSSADL model with other algorithms under varying MIs

Monitoring Interval (sec)	ETM-LWSSADL	TAAPML Model	TMM Model
	Delay (ms)		
20	35.51	40.00	43.00
40	36.16	40.66	43.87
60	36.49	41.33	44.25
80	36.62	41.61	44.78
100	37.10	42.26	45.27
	Packet Delivery Ratio		
20	99.57	99.12	97.31
40	99.76	99.40	97.69
60	99.78	99.57	98.12
80	99.82	99.60	98.34
100	99.85	99.68	98.97

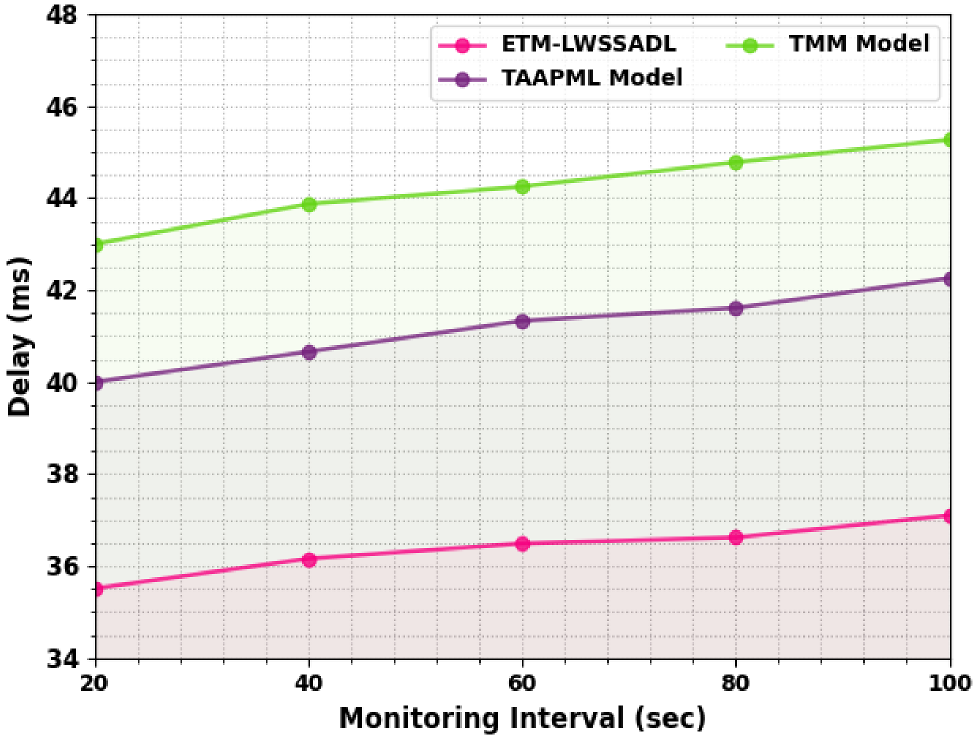

Figure 3. DEL analysis of ETM-LWSSADL model under varying MIs

In Figure 4, a brief PDR result of the ETM-LWSSADL technique is compared with respect to distinct MIs. The experimental values demonstrate that the ETM-LWSSADL technique reaches enhanced performance with maximum PDR values. With MI of 20, the ETM-LWSSADL technique offers increased PDR of 99.57 while the TAAPML and TMM models attain decreased PDR of 99.12 and 97.31 correspondingly. Also, with MI of 100, the ETM-LWSSADL approach offers enhanced PDR of 99.85 while the TAAPML and TMM models attain decreased PDR of 99.68 and 98.97 correspondingly.

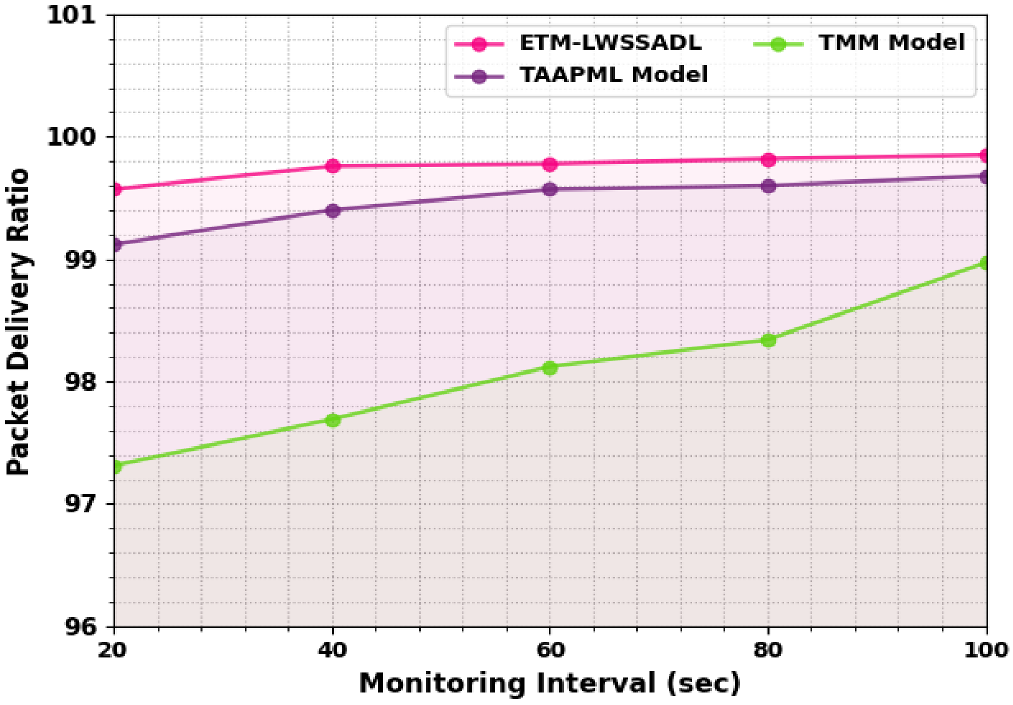

Figure 4. PDR analysis of ETM-LWSSADL model under varying MIs

In Table 2, the comparative analysis of the ETM-LWSSADL methodology is studied in terms of residual energy (RESE) and overhead (OHD).

In Figure 5, a detailed RESE outcome of the ETM-LWSSADL algorithm is compared with respect to various MIs. The simulation values implied that the ETM-LWSSADL algorithm reaches higher solution with superior RESE values. With MI of 20, the ETM-LWSSADL technique offers increased RESE of 12.01J while the TAAPML and TMM methodology obtain lesser RESE of 11.66J and 11.41J correspondingly. Moreover, with MI of 100, the ETM-LWSSADL algorithm offers increased RESE of 10.92J while the TAAPML and TMM algorithms attain minimal RESE of 10.44J and 10.28J correspondingly.

Figure 6 defines a comparative OHD result of the ETM-LWSSADL methodology under varying MIs. The figure indicates that the TMM system reaches worse performance with increased OHD values whereas the TAAPML algorithm gains somewhat decreased OHD values. But, the ETM-LWSSADL system achieves optimum results with worse OHD values of 92Kb, 195Kb, 254Kb, 318Kb, and 86Kb, correspondingly.

Table 2. RESE and OHD analysis of ETM-LWSSADL model with other algorithms under varying MIs

Monitoring Interval (sec)	ETM-LWSSADL	TAAPML Model	TMM Model
	Residual Energy (Joules)		
20	12.01	11.66	11.41
40	11.75	11.45	11.27
60	11.63	11.30	10.94
80	11.27	10.79	10.41
100	10.92	10.44	10.28
	Overhead (Kb)		
20	92	173	209
40	195	336	382
60	254	389	464
80	318	483	561
100	86	173	209

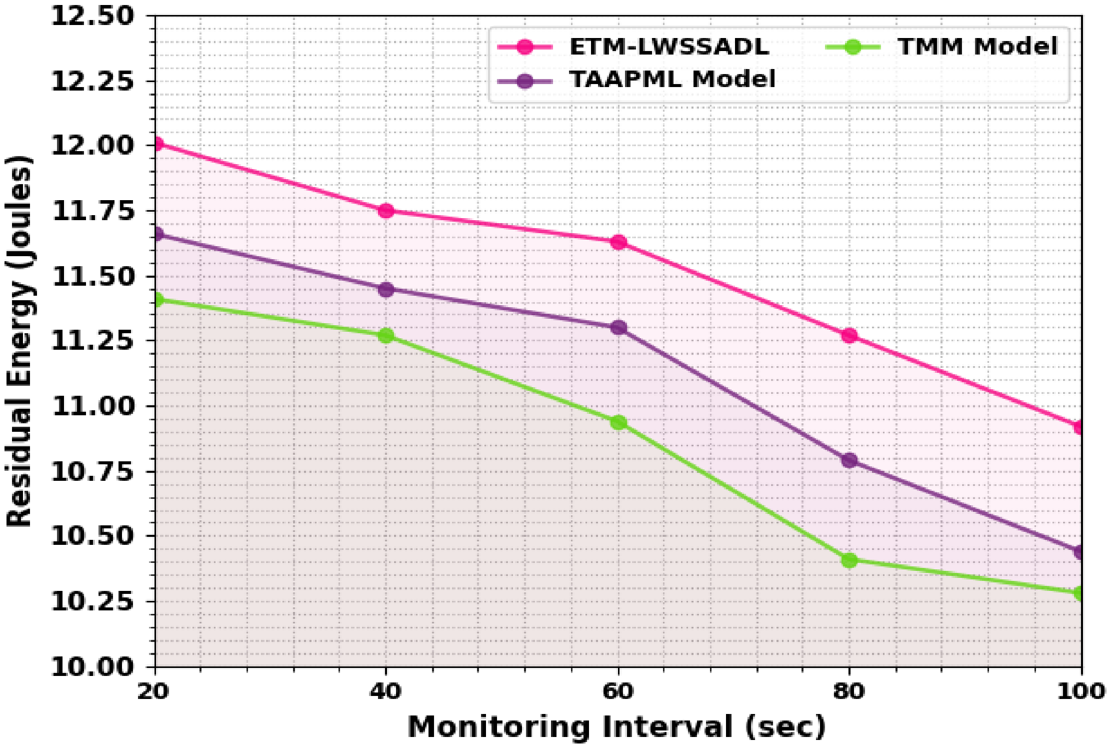

Figure 5. RESE analysis of ETM-LWSSADL model under varying MIs

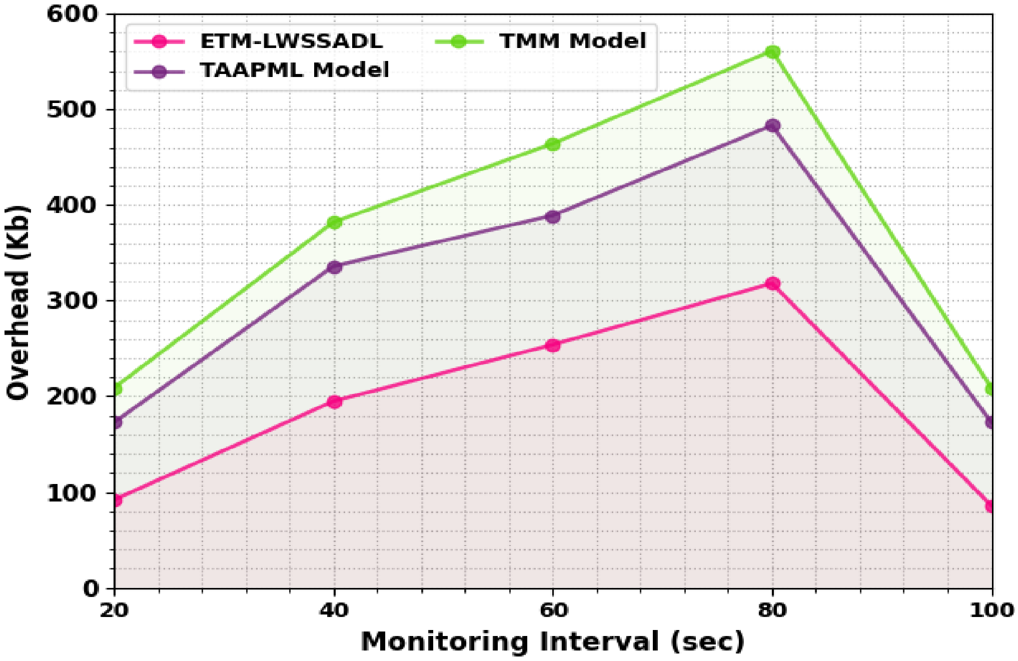

Figure 6. OHD analysis of ETM-LWSSADL model under varying MIs

In Table 3, the comparison investigation of the ETM-LWSSADL system is studied in terms of DEL and PDR.

Figure 7signifies the comparative DEL result of the ETM-LWSSADL algorithm under varying attack frequency (AF). The figure indicates that the TMM model obtains least performance with enhanced DEL values whereas the TAAPML algorithm obtains slightly reduced DEL values. Nevertheless, the ETM-LWSSADL approach obtains optimum results with least DEL values of 37.23ms, 37.41ms, 36.22ms, 36.85ms, and 37.73ms, correspondingly.

In Figure 8, a brief PDR result of the ETM-LWSSADL algorithm is compared with respect to distinct AFs. The simulation outcome exposed that the ETM-LWSSADL technique reaches enhanced solution with superior PDR values. With AF of 50Kb, the ETM-LWSSADL system offers superior PDR of 99.99 while the TAAPML and TMM models attain decreased PDR of 99.91 and 99.09 correspondingly. In addition, with AF of 150Kb, the ETM-LWSSADL technique offers increased PDR of 98.88 while the TAAPML and TMM approaches gain minimal PDR of 98.15 and 96.96 correspondingly.

Table 3. DEL and PDR analysis of ETM-LWSSADL model with other algorithms under varying AFs

Attack Frequency (Kb)	ETM-LWSSADL	TAAPML Model	TMM Model
	Delay (ms)		
50	37.23	38.90	44.18
75	37.41	38.73	44.30
100	36.22	38.22	44.52
125	36.85	38.73	45.15
150	37.73	39.18	45.38
	Packet Delivery Ratio		
50	99.99	99.91	99.09
75	99.97	99.39	98.2
100	99.77	99.02	97.35
125	99.40	98.22	97.28
150	98.88	98.15	96.96

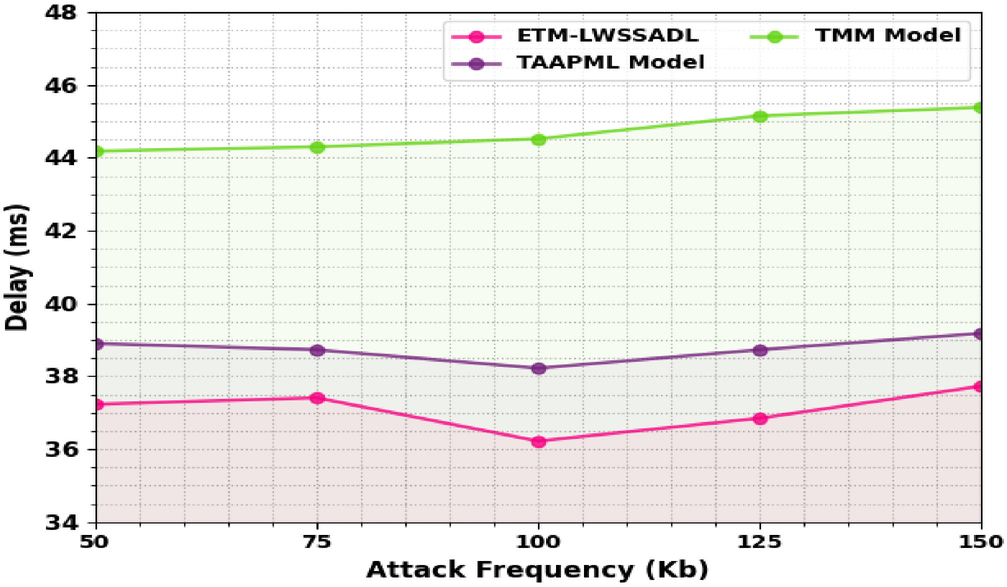

Figure 7. DEL analysis of ETM-LWSSADL model under varying AFs

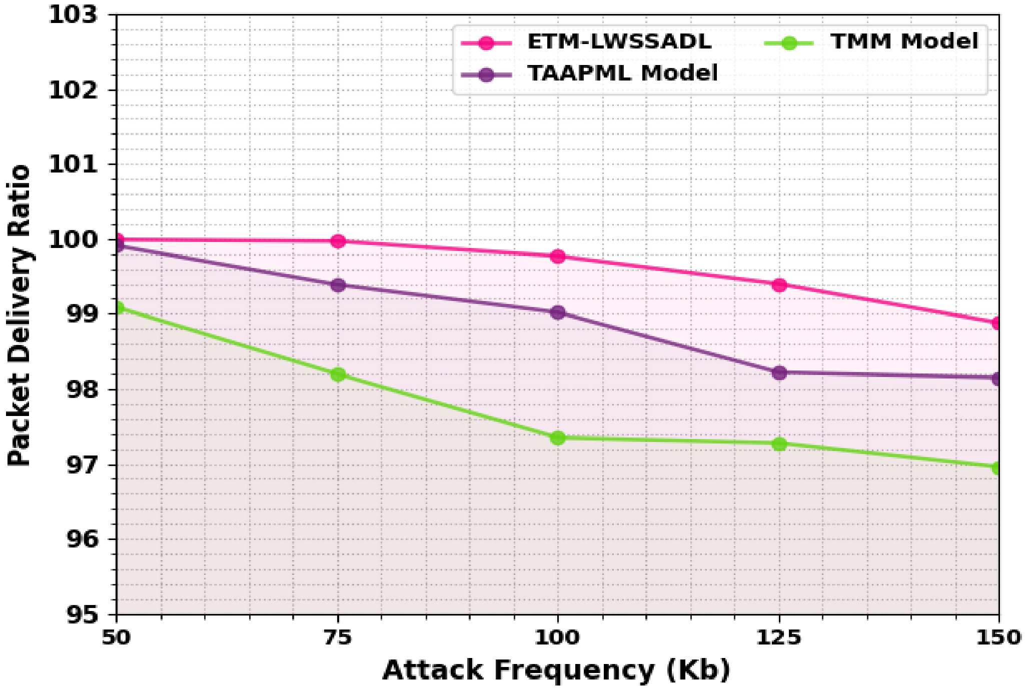

Figure 8. PDR analysis of ETM-LWSSADL model under varying AFs

In Table 4, the comparative examination of the ETM-LWSSADL method is studied with respect to RESE and OHD.

In Figure 9, a comprehensive RESE result of the ETM-LWSSADL methodology is compared under various AFs. The experimental values implied that the ETM-LWSSADL algorithm reaches improved solution with maximum RESE values. With AF of 50Kb, the ETM-LWSSADL technique offers increased RESE of 11.78J while the TAAPML and TMM system attain decreased RESE of 10.98J and 10.66J correspondingly. Moreover, with AF of 150Kb, the ETM-LWSSADL technique offers increased RESE of 12.03J while the TAAPML and TMM algorithms attain minimal RESE of 11.20J and 111.10J correspondingly.

Figure 10 exemplifies a comparative OHD outcome of the ETM-LWSSADL system under distinct AFs. The figure implied that the TMM algorithm gains least solution with higher OHD values whereas the TAAPML approach obtains some what lesser OHD values. However, the ETM-LWSSADL methodology reaches optimum results with least OHD values of 47Kb, 78Kb, 101Kb, 135Kb, and 182Kb, correspondingly.

Table 4. RESE and OHD analysis of ETM-LWSSADL model with other algorithms under varying AFs

Attack Frequency (Kb)	ETM-LWSSADL	TAAPML Model	TMM Model
	Residual Energy (Joules)		
50	11.78	10.98	10.66
75	11.79	11.11	10.87
100	11.87	11.17	10.97
125	11.92	11.17	11.07
150	12.03	11.20	11.10
	Overhead (Kb)		
50	47	86	144
75	78	136	244
100	101	178	332
125	135	232	376
150	182	278	452

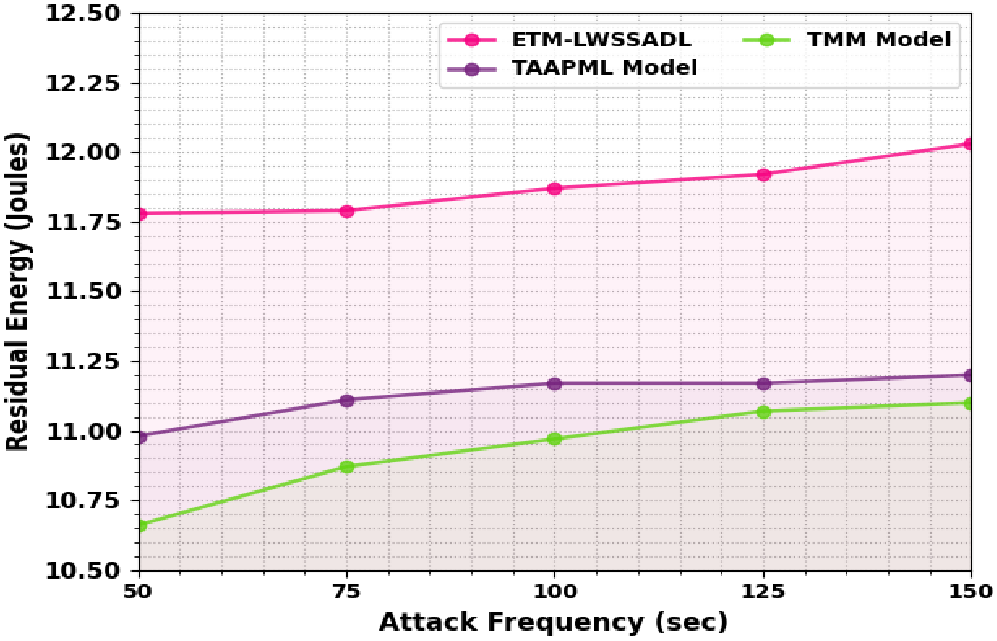

Figure 9. RESE analysis of ETM-LWSSADL model under varying AFs

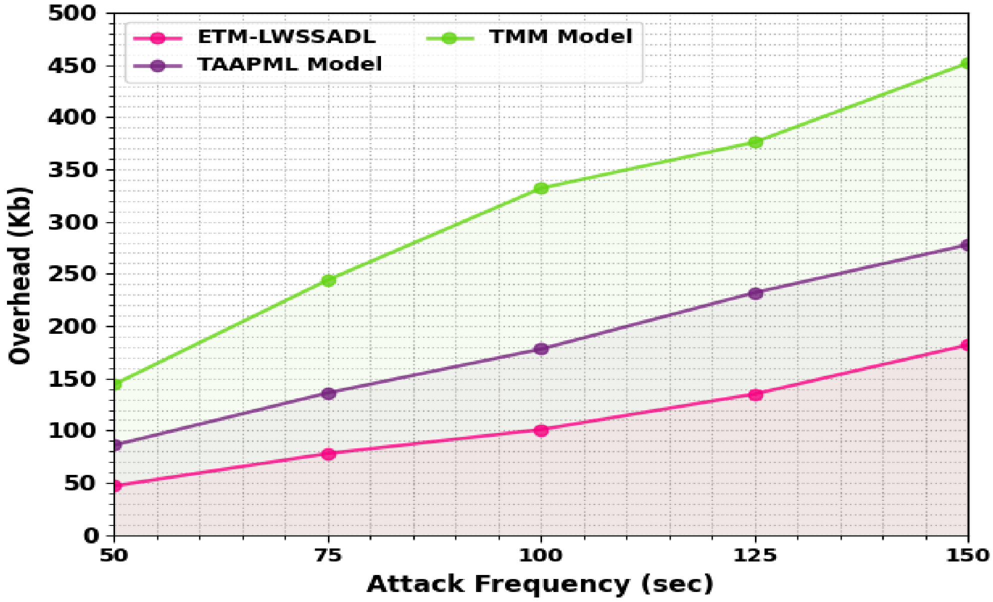

Figure 10. OHD analysis of ETM-LWSSADL model under varying AFs

Thus, the ETM-LWSSADL technique can be used to attain maximum trust in the SIoT networks.

CONCLUSION

In this study, we have developed an ETM-LWSSADL technique for SIoT Networks. The ETM-LWSSADL technique computes direct and indirect trust values and is assessed depending upon different weighing factors for maximizing the application performance and creating a secure data transmission process. During authentication process, when the SIoT device with TTV is not greater than THV or authentication token is invalid, the gateways then disregard the node. Besides, the BiGRU model is applied to generate a THV on collected traffic data. Moreover, the ETM-LWSSADL technique exploits the LWSSA technique for optimum hyper parameter selection of the BiGRU approach. To highlight the enhanced performance of the ETM-LWSSADL algorithm, an extensive range of simulations can be involved. The experimental values highlighted that the ETM-LWSSADL technique gains maximum performance over other models. The results of the experiments showed that the ETM-LWSSADL algorithm achieves a better solution with the highest possible RESE values. With an AF of 50Kb, the ETM-LWSSADL method achieves a higher RESE of 11.78J, compared to the 10.98J and 10.66J achieved by the TAAPML and TMM systems, respectively. In addition, the ETM-LWSSADL method achieves a minimal RESE of 111.10J and an enhanced RESE of 12.03J with an AF of 150Kb, while the TAAPML and TMM algorithms achieve minimal RESEs of 11.20J and 11.20J, respectively.

Funding: The authors declare they have no funding applied.
Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

1. Xiang X, Cao J, Fan W, Xiang S, Wang G. Blockchain enabled dynamic trust management method for the internet of medical things.Decis. Support Syst., 2024; 114184. DOI:10.1016/j.dss.2024.114184
2. Souri A, Zhao Y, Gao M, Mohammadian A, Shen J, Al-Masri E. A trust-aware and authentication-based collaborative method for resource management of cloud-edge computing in social internet of things.IEEE Trans. Comput. Soc. Syst. 2023.https://doi.org/10.1109/TCSS.2023.3241020
3. Rizwanullah M, Singh S, Kumar R, Alrayes FS, Alharbi A, Alnfiai MM, et al. Development of a Model for Trust Management in the Social Internet of Things.Electronics.2022;12(1):41.http://dx.doi.org/10.3390/electronics12010041
4. Dayyani A, Abbaspour M. SybilPSIoT: Preventing Sybil attacks in signed social internet of things based on web of trust and smart contract.IET Commun. 2024.https://doi.org/10.1049/cmu2.12734
5. Bangui H, Buhnova B, Kusnirakova D. Halasz D. Trust management in social Internet of Things across domains.Internet of Things. 2023; 100833.http://dx.doi.org/10.1016/j.iot.2023.100833
6. Alalwany E, Mahgoub I. Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions.Sens.2024;24(2):368.https://doi.org/10.3390/s24020368
7. Kalimuthu VK, Velumani R. Modeling of Intrusion Detection System Using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment. Braz Arch Biol Technol. 2024;67. https://doi.org/10.1590/1678-4324-2024231010.
8. Amiri-Zarandi M, Dara RA, Fraser E. LBTM: A lightweight blockchain-based trust management system for social internet of things.J.Supercomput. 2022;1-19.https://link.springer.com/article/10.1007%2Fs11227-021-04231-3
9. Zhao M, Shi C, Yuan Y. Blockchain-Based Lightweight Authentication Mechanisms for Industrial Internet of Things and Information Systems. Int. J. Semant. Web Inf. Syst.2024; 20(1):1-30.http://dx.doi.org/10.4018/IJSWIS.334704
10. Rehman A, Awan KA, Ud Din I, Almogren A, Alabdulkareem M. FogTrust: Fog-Integrated Multi-Leveled Trust Management Mechanism for Internet of Things. Tech. 2023; 11(1):27.http://dx.doi.org/10.3390/technologies11010027
11. Cheng G, Wang Y, Deng S, Xiang Z, Yan X, Zhao P, et al. A Lightweight Authentication-Driven Trusted Management Framework for IoT Collaboration. EEE Trans. Serv. Comput. 2024.http://dx.doi.org/10.1109/TSC.2023.3349305
12. Abdelghani W, Amous I, Zayani CA, Sèdes F, Roman-Jimenez G. Dynamic and scalable multi-level trust management model for Social Internet of Things.J.Supercomput. 2022; 78(6):8137-93.https://link.springer.com/article/10.1007%2Fs11227-021-04205-5
13. Roy SS, Sahu BJR, Dash S. Enhanced trust management for building trustworthy social internet of things network.IET Netw. 2023.http://dx.doi.org/10.1049/ntw2.12111
14. Kumar KV, Balakrishnan S. Multi-objective Sand Piper Optimization Based Clustering with Multihop Routing Technique for IoT Assisted WSN. Braz Arch Biol Technol. 2023;66. https://doi.org/10.1590/1678-4324-2023220866.

15. Spoljaric T, Pavić I, Alinjak T. Performance Comparison of No-preference and Weighted Sum Objective Methods in Multi-Objective Optimization of AVR-PSS Tuning in Multi-machine Power System. Tech Vjesn. 2022;29(6):1931-1940. https://doi.org/10.17559/TV-20211216115635.
16. Basha PH, Prathyusha G, Rao DN, Gopikrishna V, Peddi P, Saritha V. AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks.IJISAE. 2024; 12(1s):361-74.
17. Velumani R, Kumar KV. Barnacles Mating Optimizer with Hopfield Neural Network Based Intrusion Detection in Internet of Things Environment. Tech Vjesn. 2023;30(6):1821-1828. https://doi.org/10.17559/TV-20211216115635.237:110048.
18. Meena Kowshalya A, Valarmathi ML. Dynamic trust management for secure communications in social internet of things (SIoT). Sādhanā. 2018; 43(9):136.http://dx.doi.org/10.1007/s12046-018-0885-z
19. Avcı İ, Yıldırım M. Solving Weapon-Target Assignment Problem with Salp Swarm Algorithm. Tech Vjesn. 2023;30(1):17-23. https://doi.org/10.17559/TV-20211216115635.
20. Jegatheesan D, Arumugam C. SIoV-FTFSA-CAOA: a fuzzy trust-based approach for enhancing security and energy efficiency in social internet of vehicles. Wireless Networks, 2024; 1-20.http://dx.doi.org/10.1007/s11276-023-03626-9
21. Balakrishnan S, Kumar KV. Hybrid Sine-Cosine Black Widow Spider Optimization based Route Selection Protocol for Multihop Communication in IoT Assisted WSN. Tech Vjesn. 2023;30(4). https://doi.org/10.17559/TV-20211216115635.