Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028088
Article

Tech Science Press

Statistical Analysis with Dingo Optimizer Enabled Routing for Wireless Sensor Networks

Abdulaziz S. Alghamdi[1,*], Randa Alharbi[2], Suliman A. Alsuhibany[3] and Sayed Abdel-Khalek[4,5]

[1]Department of Mathematics, College of Science & Arts, King Abdulaziz University, Rabigh, 21911, Saudi Arabia
[2]Department Statistics, College of Science, University of Tabuk, Tabuk, Saudi Arabia
[3]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia
[4]Department of Mathematics and Statistics, College of Science, Taif University, Taif, 21944, Saudi Arabia
[5]Mathematics Department, Faculty of Science, Sohag University, Sohag, 82524, Egypt
*Corresponding Author: Abdulaziz S. Alghamdi. Email: ashalghamedu@kau.edu.sa
Received: 02 February 2022; Accepted: 17 March 2022

Abstract: Security is a vital parameter to conserve energy in wireless sensor networks (WSN). Trust management in the WSN is a crucial process as trust is utilized when collaboration is important for accomplishing trustworthy data transmission. But the available routing techniques do not involve security in the design of routing techniques. This study develops a novel statistical analysis with dingo optimizer enabled reliable routing scheme (SADO-RRS) for WSN. The proposed SADO-RRS technique aims to detect the existence of attacks and optimal routes in WSN. In addition, the presented SADO-RRS technique derives a new statistics based linear discriminant analysis (LDA) for attack detection, Moreover, a trust based dingo optimizer (TBDO) algorithm is applied for optimal route selection in the WSN and accomplishes secure data transmission in WSN. Besides, the TBDO algorithm involves the derivation of the fitness function involving different input variables of WSN. For demonstrating the enhanced outcomes of the SADO-RRS technique, a wide range of simulations was carried out and the outcomes demonstrated the enhanced outcomes of the SADO-RRS technique.

Keywords: Statistical analysis; reliability; routing; wireless sensor networks; linear discriminant analysis; dingo optimizer; security

1 Introduction

In recent times, WSN has extended the application range from early deployment for battlefield intelligence surveillance to fields like meteorological weather forecasting, emergency response support, factory automation security application, and so on. WSN consists of inexpensive and small sensors without a current architecture [1]. They are frequently utilized for sensing, processing, transmitting, and receiving data from the region they are positioned beforehand it is transported to a base station. A conventional WSN contains several sensors that are classified based on the environment and the structure (topology) where they are deployed. Basically, WSN is classified based on the deployment

of the sensors in the environment [2]. This node is of equivalent capacity, while others have different capacities, based on the infrastructure. The three major kinds type WSN architecture are hierarchical, flat-based (tree), and cluster-based. Moreover, the environment where the sensors are positioned in a WSN is classified into five groups, such as mobile WSN, underground WSN, terrestrial WSN, underwater WSN, and multimedia WSN system [3]. The sensors in a WSN are frequently deployed in inaccessible, remote, and harsh regions and are frequently represented by resource constraints including limited storage, limited power, short communication range, and limited bandwidth [4]. They are integrated with the susceptibility of the wireless medium (that is open and shared) have generated sensors vulnerable to distinct security attacks namely the denial of service (DoS) [5]. Fig. 1 illustrates the WSN structure.

Even though conventional security approaches like authentication and cryptography could offer security at certain level, they alone could not handle compromised node attacks [6]. When the nodes are compromised, it launches attacks based on commands from the outside that could control or cripple the entire WSN system. For instance, malicious node could attract the information from another node via distinct method, and when it begins to receive the information, it could randomly receive or drop all information that considerably reduces the routing system efficiency [7]. To handle this type of node is to detect and monitor them. While there are no centralized authorities in WSN, nodes must detect and monitor malicious nodes in a distributed way. Several solutions are presented for securing WSN [8], together with routing. Since routing executes data distribution to BS, it is major protocol for WSN. Therefore, secured routing is strong against packet drop and disruption, and alteration act on routing process is vital [9,10]. To protect routing, particularly against compromised nodes, several solutions have been introduced. One of these solutions is trust establishment, utilized in several study areas. Trust establishment identifies untrustworthy and trustworthy nodes by estimating them according to past performance or behavior. It prevents untrustworthy nodes and only chooses trustworthy in routing process [11]. As trust method is efficient and simple in compromised node detection, a considerable study is performed for enhancing cooperation and improving security in the networks.

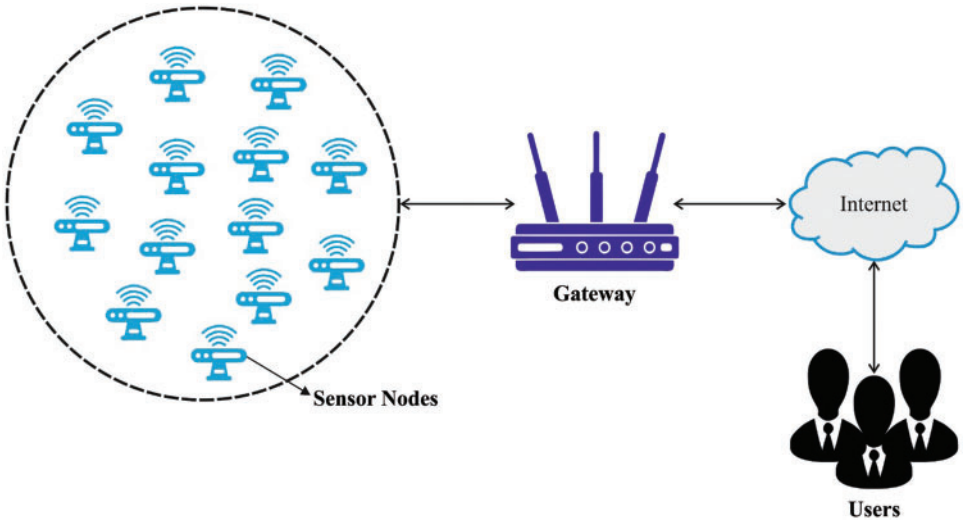

Figure 1: WSN structure

Rathee et al. [12], proposed an ACO based QoS aware energy balancing secured routing (QEBSR) approach for WSN. Improved heuristics to calculate the end-to-end delay of communication and the

trust factor of the node on the routing path are presented. The presented method has been related to 2 current approaches: energy efficient routing with node compromised resistance and distributed energy balanced routing. Haseeb et al. [13] developed an energy-effective and secured routing method (ESR) for avoiding intrusion from IoT based WSN to improve the data trustworthiness and network period. First, the presented method makes distinct energy-effective clusters based on the intrinsic qualify of nodes. Next, according to the (k,n) threshold-based Shamir secret sharing system, the security and reliability of the sensory data amongst the BS and CH are accomplished.

Haseeb et al. [14] presented an intrusion prevention architecture for mobile IoT devices using the incorporation of WSN for providing data security with enhanced network delivery ratio. The presented method is comprised of two sub-elements. First, autonomously organized and non-overlapping clusters are created and sustained the clusters stability according to the uncertainty principle. Next, end-to-end secured and multihop routing path is designed according to the blockchain architecture. In Selvi et al. [15], a secured routing method named energy aware trust based secured routing approach is presented whereby the trust score assessment is utilized for identifying the malevolent user efficiently in WSN and spatio-temporal constraint is utilized with DT approach to choosing optimal path.

This study develops a novel statistical analysis with dingo optimizer enabled reliable routing scheme (SADO-RRS) for WSN. The proposed SADO-RRS technique aims to detect the existence of attacks and optimal routes in WSN. In addition, the presented SADO-RRS technique derives a new statistics based linear discriminant analysis (LDA) for attack detection, Moreover, a trust based dingo optimizer (TBDO) algorithm is applied for optimal route selection in the WSN and accomplishes secure data transmission in WSN. Besides, the TBDO algorithm involves the derivation of the fitness function involving different input variables of WSN. In order to demonstrate the enhanced outcomes of the SADO-RRS technique, a wide range of simulations was carried out.

2 The Proposed Model

In this study, a novel SADO-RRS technique has been developed for reliable routing in WSN. The proposed SADO-RRS technique determines the presence of attacks and optimal routes in WSN. In addition, the presented SADO-RRS technique derives a new statistics based LDA for attack detection. Furthermore, a TBDO algorithm is applied for optimal route selection in the WSN and accomplishes secure data transmission in WSN.

2.1 LDA Based Attack Detection

Primarily, the LDA model is applied for the detection of intrusions in the network. The discriminant analysis concentrates on the connection amongst several independent variables and definite dependence variables by creating multiple independent variables. This kind of multivariate investigation defines the extents of the sum of composite variables discriminate amongst more than two existing sets of subjects and also could develop the classifier model to predict the group membership of novel observation. During this case, a linear discriminant function (LDF) which passed with the means of 2 groups (centroids) are utilized for discriminating subjects amongst 2 centroids. If there are further centroids, the amount of centroid minus one purpose has been required for classifying an observation amongst them. In order to all centroids, LDA considers as the explanatory variable that is usually distributed with equivalent covariance matrices. To all cases, the evaluated co-efficient to independent variables are multiplied by case's score on that variables.

The LDF has been demonstrated as:

$$LDF = b_0 + b_1 x_{i1} + b_2 x_{i2} + \cdots + b_k x_{ik} = bX, \tag{1}$$

where b_j implies the value of j^{th} co-efficient, $j = 1, \ldots, k$, and χ_{ij} stands for the value of i^{th} cases of j^{th} predictors. The LDF is also be expressed in standardization procedure that permits relating variables to measure on various scales. The co-efficient with huge absolute values reflect superior discriminate capability to its equivalent variable [16]. In the *LDF* score is evaluate forecasted probability and forecasted centroid membership to all cases on the dependent variable. This technique was dependent upon the rationale which it can be further possible that independent as well as dependent variables have been compared to the amongst-centroids sum of square are superior comparative to within-centroid sum of squares. Likewise, the ratio of amongst-centroids divided by entire amount of squares (eta-squared statistic or solved variabilities) or of within-centroid divided by entire amount of squares (Wilks' lambda statistic or unsolved variabilities) has been utilized for assessing the connection. As noted, the ratio of amongst-centroid divided by within-centroid amount of squares are analogue to ratio of variances that is F statistic, testing which controls the possibilities which the detected connection is because of chances.

The rule by that the discriminant co-efficient (or weights) were chosen is that maximizing the distance amongst 2 centroid means (centroids) $|\overline{y}_1 - \overline{y}_2|$. The fisher is initially proposed to alter the multivariate observation x for univariate observation y just as y's resulting from centroids 1 and 2 are the maximal distance amongst them. Therefore, the linear group $y = a'x$ is the one which maximizes the ratio (squared distance amongst instance means)/(instance variance y). The vector of co-efficient is provided as the eigenvectors of matrix $* S^{-1}$, whereas $B = (\overline{x}_1 - \overline{x}_2)'$ implies the amongst-centroid matrix and S refers the evaluation of Σ. Extremely important features of this composite amount of squares are that it is enclosed the variabilities and the co-variabilities of all the variables. The discriminant co-efficient is computed from unstandardized or standardized procedure however it can be irrelatively of procedure, minimum informative than individuals from regression. Considering that there are 2 centroids, $\overline{x}_1, \overline{x}_2$ refers the means of all the centroids, and S implies the pooled covariance matrix, the distribution rule dependent upon Fisher's discriminant function is subsequent:

$$X_i \in \begin{cases} group1, if\ y = (\overline{x}_1 - \overline{x}_2)' S^{-1} X_i \geq \dfrac{1}{2} (\overline{x}_1 - \overline{x}_2)'^{S^{-1}} (\overline{x}_1 + \overline{x}_2), \\ group2, if\ y = (\overline{x}_1 - \overline{x}_2)' S^{-1} X_i < \dfrac{1}{2} (\overline{x}_1 - \overline{x}_2)'^{S^{-1}} (\overline{x}_1 + \overline{x}_2) \end{cases} \tag{2}$$

2.2 TBDO Based Routing Technique

The dingoes are sufficient able for finding the place of prey. Afterward trace the place, the pack after that alpha surrounds the prey. For modeling dingo's social hierarchy, it can be considered that the present optimum agent's method is an objective or purpose prey that is same as the optimum as the quest region is not recognized a priori [17]. Meanwhile, another quest agency is until seek for refreshing its approaches on the following feasible method. This performance of dingoes is demonstrated as the subsequent mathematical Eqs. (3)–(7). Besides, a brief explanation of nomenclatures is utilized from the formula.

$$\vec{D}_d = |\vec{A} \cdot \vec{P}(x) - \vec{P}(i)|, \tag{3}$$

$$\vec{P}(i+1) = \vec{P}_p(i) - \vec{B} \cdot \vec{D}(d), \tag{4}$$

$$\vec{A} = 2 \cdot \vec{a}_1, \tag{5}$$

$$\vec{B} = 2\vec{b} \cdot \vec{a}_2 - \vec{b}, \tag{6}$$

$$\vec{b} = 3 - \left(I * \left(\frac{3}{I_{\max}} \right) \right). \tag{7}$$

The place of neighborhood dingoes is signified utilizing a 2D place vector. Based on the place of prey (P^*, Q^*), a dingo is upgraded their place at the location of (P, Q). Every feasible place is marked from the diagram nearby the optimum agents, regarding the present place as altering the value of $\vec{A}$ and $\vec{B}$ vectors. For instance, by setting $\vec{A} = (1, 0)$ and $\vec{B} = (1, 1)$, dingo is attained at $(P^* - P, Q^*)$. It also signifies utilizing 3D space. It can be obviously demonstrated that arbitrary vectors a1 and a2 allow dingoes for entering someplace amongst the points. Eqs. (3) and (4) support dingoes for changing their places inside the quest region nearby the prey from several arbitrary places. For reaching a search space with N dimensional, similar formulas are utilized and the dingo will move in hypercube about the optimum outcome done to this point.

Conversely, during the searching space based on the model, agent does not usually have computation of place of the prey (optimally). Scheming the dingoes hunting plan mathematical, it is considered that each pack member containing alpha, beta, and others are optimum skill on the potential place of prey. The alpha dingo continuously commands the hunting. But, at times beta and other dingo's can also be participating from hunting. Therefore, it is assumed the 1st two optimum values attained so far. According to place of optimum searching agents, other dingoes are also required for updating their place. Due to the discussion, Eqs. (8)–(16) are demonstrated this issue. In addition, a brief explanation of the nomenclatures utilized in the formula.

$$\vec{D}_\alpha = \left| \vec{A}_1 \cdot \vec{P}_\alpha - \vec{P} \right|, \tag{8}$$

$$\vec{D}_\beta = \left| \vec{A}_2 \cdot \vec{P}_\beta - \vec{P} \right|, \tag{9}$$

$$\vec{D}_o = \left| \vec{A}_3 \cdot \vec{P}_o - \vec{P} \right|, \tag{10}$$

$$\vec{P}_1 = \left| \vec{P}_\alpha - \vec{B} \cdot \vec{D}_\alpha \right|, \tag{11}$$

$$\vec{P}_2 = \left| \vec{P}_\beta - \vec{B} \cdot \vec{D}_\beta \right|, \tag{12}$$

$$\vec{P}_3 = \left| \vec{P}_o - \vec{B} \cdot \vec{D}_o \right|. \tag{13}$$

For calculating the intensity of all the dingoes, subsequent formulas are being utilized:

$$\vec{I}_\alpha = \log \left(\frac{1}{F_\alpha - (1E - 100)} + 1 \right), \tag{14}$$

$$\vec{I}_\beta = \log \left(\frac{1}{F_\beta - (1E - 100)} + 1 \right), \tag{15}$$

$$\vec{I}_o = \log \left(\frac{1}{F_o - (1E - 100)} + 1 \right). \tag{16}$$

The place upgrade from the $2D$ searching space. It is easily visualization the place upgrade of alpha, beta, and other dingoes. It is also assumed that dingoes (alpha, beta, and others) upgrade their places arbitrarily and compute the place of prey from the searching space.

When there is no place upgrade, it refers the dingo done the hunting by attacking the prey. In order to mathematical formulate the approach, the value of $\vec{b}$ has reduced linearly. The point stated that the change range of $\vec{D}_\alpha$ is also reduced by $\vec{b}$. It is also be recognized as $\vec{D}_\alpha$ that is an arbitrary value from the $[-3b, 3b]$ interval where b has been decreased in three to zero under the iterations. If the arbitrary values of $\vec{D}_\alpha$ are in one and one, a searching agent next place possibly from someplace amongst their present and the prey place. Fig. 2 illustrates the flowchart of DO technique [18].

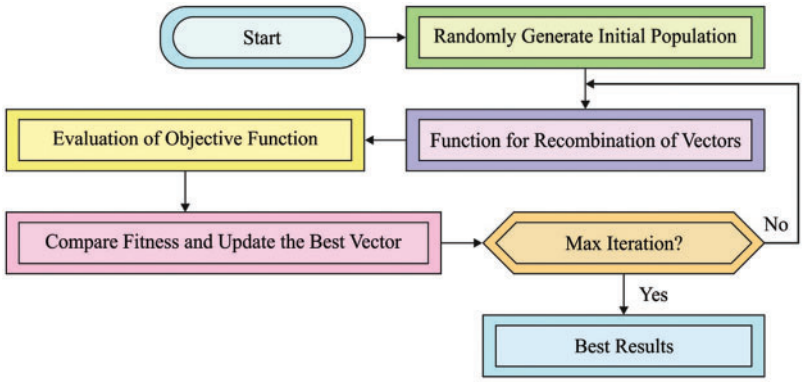

Figure 2: Flowchart of DO technique

The presented surrounding technique does certainly reveal exploration to any extent; but, for accentuating exploration, DOX needs further operation. The DOX supports their quest agent from changing its place dependent upon the locating of, β, others, and the targeted prey. Even, with this operator, the DOX is inactivating local solutions.

The dingoes hunt the prey frequently based on the pack's place. It is continuously travel forwarded to hunt and strike predators. So, B has been utilized to arbitrary values where once the value has lesser than -1, it refers the prey has moving outside the searching agent, however when the value has superior to 1, it signifies the pack techniques the prey. This intervention supports the DOX for scanning the target generally. For determining that prey is optimum suitable that 1 assumes dingoes avoided the predator. Another element of DOX which creates exploration possible is A. In Eq. (5), the vector A is create some arbitrary number amongst zero and three, to an arbitrary prey weight. The DOX implies the stochastic function, considered as vector ≤ 1 preceded than ≥ 1 for explaining the effect of gap expressed in Eq. (3).

It is optimum to search and avoidance of neighboring optimal. According to a dingo's place, it can be arbitrarily agreed on prey value and create it essential for meeting dingo rigidly/beyond. Purposely, it is utilized A for providing stochastic exploration value in the primary to last iterations. This technique has effective from protect the solution at local optimum. At last, the DOX ends themselves when it meets the end condition.

The presented approach develops a FF utilizing 3 input parameters such as trust level, distance to neighbors, and energy to optimum route selective.

Distance to neighbors: It is suitable to select route with lesser distance amongst neighbouring nodes. In the intra-cluster communication procedure, sensor node utilization power to data broadcast. When the neighbour node distance has been moderated, then the power of intra-cluster broadcast is also minimized.

Objective 1: Minimizing

$$f_1 = \sum_{j=1}^{m} \frac{1}{l_j} \left(\sum_{i=1}^{l_j} dis\left(CH_j, s_i\right) \right) \tag{17}$$

Trust factor (TF): Initially, every node is declared that TF is one. The value of TF has been reduced by anomalous prediction method if the node processes the abnormal task and nodes are named as malicious nodes.

Objective 2: Maximizing

$$f_2 = \sum_{j=1}^{m} \frac{1}{m} \left(TF_j\right) \tag{18}$$

Energy: When the node intake minimal power utilized as sensing, process, and transmission process also with maximal RE has gathered of minimal energy ratio. So, the low as energy ratio, the CH selective develop more possible.

Objective 3: Minimizing

$$f_3 = \sum_{j=1}^{m} \frac{E_c\left(CH_j\right)}{E_R\left(CH_j\right)} \tag{19}$$

In the proposed technique, it could be vital to decrease the linear group of main functions. So, the potential energy function of presented approach was implemented as:

$$Minimize\ Potiential\ energy\ function = \alpha_1 \times f_1 + \alpha_2 \times f_2 + \alpha_3 \times f_3 \tag{20}$$

where $\alpha_1 + \alpha_2 + \alpha_3 = 1, \alpha_2 \geq (\alpha_1 + \alpha_3)$. *Also* $0 < f_1, f_2, f_3 < 1$.

3 Experimental Validation

This section inspects the performance validation of the SADO-RRS technique with existing techniques. The results are inspected interms of distinct aspects.

Tab. 1 provides detailed intrusion detection results of the SADO-RRS technique with recent methods. Fig. 3 inspects the $prec_n$ analysis of the SADO-RRS technique with compared methods. The figure reported that the SVM model has resulted in least $prec_n$ of 0.6758. Followed by, the SOM and ANN-IDS models have obtained slightly enhanced $prec_n$ values of 0.7432 and 0.7948 respectively. In line with, the DMN-NB, GAN, and DELM techniques have accomplished moderately closer $prec_n$ values of 0.8021, 0.8531, and 0.8964 respectively. However, the SADO-RRS model has attained maximum $prec_n$ of 0.9313.

Table 1: Result analysis of SADO-RRS technique with recent approaches interms of various measures

Methods	Precision	Recall	Accuracy
SVM	0.6758	0.7111	0.6950
SOM	0.7432	0.7732	0.7550
ANN-IDS	0.7948	0.8313	0.8120
DMN-NB	0.8021	0.8283	0.8150

(Continued)

Table 1: Continued

Methods	Precision	Recall	Accuracy
GANs	0.8531	0.8830	0.8650
DELM	0.8964	0.9310	0.9123
SADO-RRS	0.9313	0.9546	0.9437

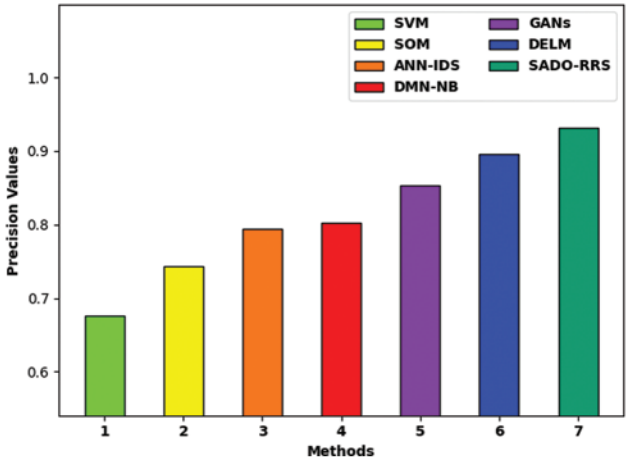

Figure 3: *Prec*$_n$ analysis of SADO-RRS technique with recent methods

Fig. 4 examines the *reca*$_l$ analysis of the SADO-RRS technique with compared methods. The figure exposed that the SVM model has resulted to least *reca*$_l$ of 0.7111. Then, the SOM and ANN-IDS systems have obtained slightly enhanced *reca*$_l$ values of 0.7732 and 0.8313 correspondingly. Likewise, the DMN-NB, GAN, and DELM techniques have accomplished moderately closer *reca*$_l$ values of 0.8283, 0.8830, and 0.9310 correspondingly. But, the SADO-RRS method has attained higher *reca*$_l$ of 0.9546.

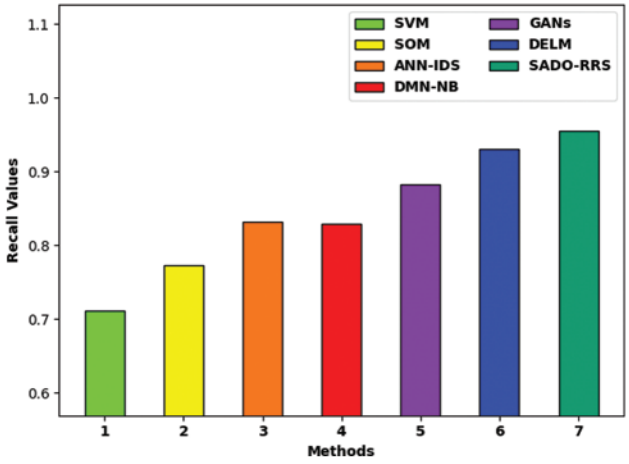

Figure 4: *Reca*$_l$ analysis of SADO-RRS technique with recent methods

Fig. 5 demonstrates the acc_y analysis of the SADO-RRS technique with compared methods. The figure outperformed that the SVM methodology has resulted in minimal acc_y of 0.6950. Afterward, the SOM and ANN-IDS techniques have obtained somewhat increased acc_y values of 0.7550 and 0.8120 correspondingly. Besides, the DMN-NB, GAN, and DELM techniques have accomplished moderately closer acc_y values of 0.8150, 0.8650, and 0.9123 correspondingly. At last, the SADO-RRS model has attained superior acc_y of 0.9437.

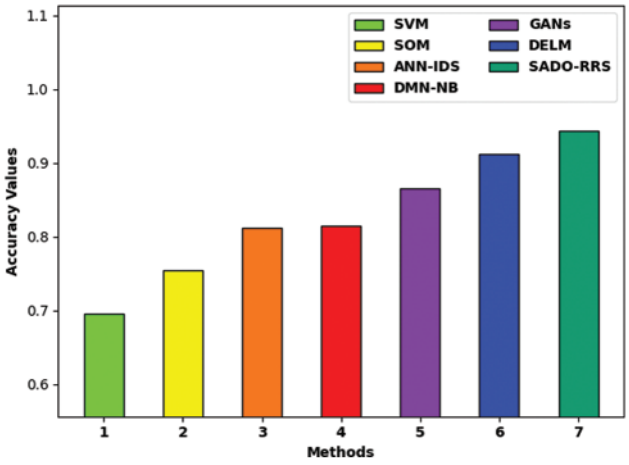

Figure 5: Acc_y analysis of SADO-RRS technique with recent methods

Tab. 2 and Fig. 6 illustrate the network lifetime (NLFT) examination of the SADO-RRS technique with existing ones under distinct number of compromised nodes. The results indicated that the SADO-RRS technique has resulted in increased NLFT over the other methods under all compromised nodes. For instance, with 5% of compromised nodes, the SADO-RRS technique has offered higher NLFT of 961 rounds whereas the DEBR, EENC, and QEBSR techniques have attained lower 793, 878, and 927 rounds respectively. Similarly, with 30% of compromised nodes, the SADO-RRS approach has obtainable maximal NLFT of 919 rounds whereas the DEBR, EENC, and QEBSR methodologies have attained lower 615, 766, and 868 rounds correspondingly.

Table 2: Network lifetime analysis of SADO-RRS technique under distinct compromised nodes

Network lifetime (Rounds)				
Compromised nodes (%)	DEBR	EENC	QEBSR	SADO-RRS
5	793	878	927	961
10	749	858	912	958
20	697	810	880	932
30	615	766	868	919

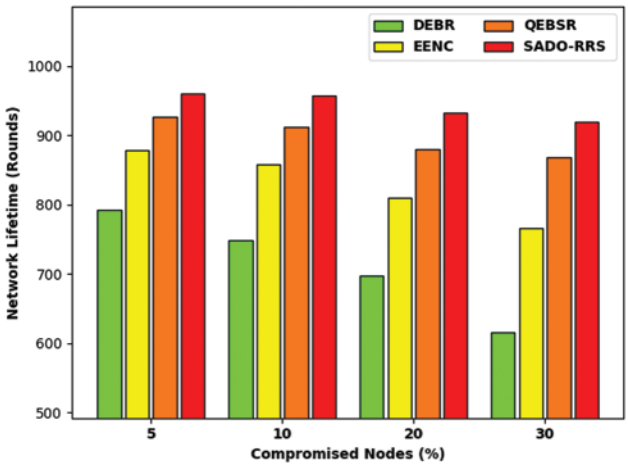

Figure 6: NLFT analysis of SADO-RRS technique under distinct compromised nodes

Tab. 3 and Fig. 7 depict the NLFT examination of the SADO-RRS approach with existing ones under distinct number of nodes. The outcomes referred that the SADO-RRS methodology has resulted in increased NLFT over the other methods under all nodes. For instance, with 100 nodes, the SADO-RRS approach has accessible maximal NLFT of 1040 rounds whereas the DEBR, EENC, and QEBSR systems have obtained minimal 693, 827, and 888 rounds correspondingly. At the same time, with 400 nodes, the SADO-RRS approach has obtainable superior NLFT of 2439 rounds whereas the DEBR, EENC, and QEBSR methodologies have reached minimal 1976, 2098, and 2360 rounds correspondingly.

Table 3: Network lifetime analysis of SADO-RRS technique under count of nodes

Network lifetime (Rounds)				
No. of nodes	DEBR	EENC	QEBSR	SADO-RRS
100	693	827	888	1040
200	1100	1228	1386	1599
400	1976	2098	2360	2439

Tab. 4 and Fig. 8 depict the PDR examination of the SADO-RRS technique with existing ones under distinct count of compromised nodes. The results referred that the SADO-RRS technique has resulted in maximum PDR over the other methods under all compromised nodes. For instance, with 5% of compromised nodes, the SADO-RRS system has offered increased PDR of 0.9670 rounds whereas the DEBR, EENC, and QEBSR systems have reached lesser of 0.9363, 0.9617, and 0.9649 rounds correspondingly. Also, with 30% of compromised nodes, the SADO-RRS approach has obtainable increased PDR of 0.9572 rounds whereas the DEBR, EENC, and QEBSR approaches have achieved reduced 0.9369, 0.9418, and 0.9480 rounds correspondingly.

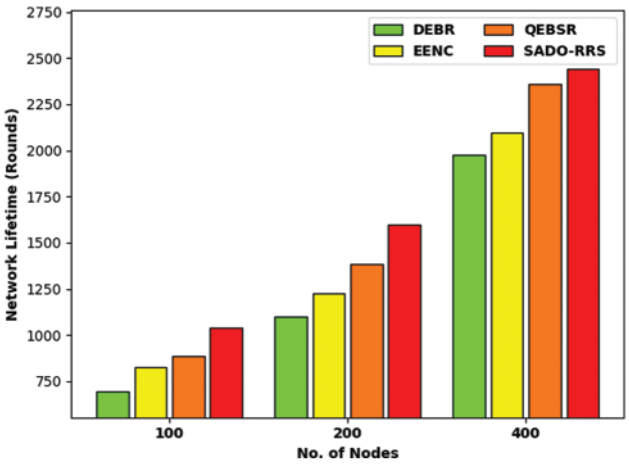

Figure 7: NLFT analysis of SADO-RRS technique under count of nodes

Table 4: PDR analysis of SADO-RRS technique under distinct compromised nodes

Packet delivery ratio				
Compromised nodes (%)	DEBR	EENC	QEBSR	SADO-RRS
5	0.9363	0.9617	0.9649	0.9670
10	0.9418	0.9599	0.9607	0.9653
20	0.9457	0.9560	0.9580	0.9634
30	0.9369	0.9418	0.9480	0.9572

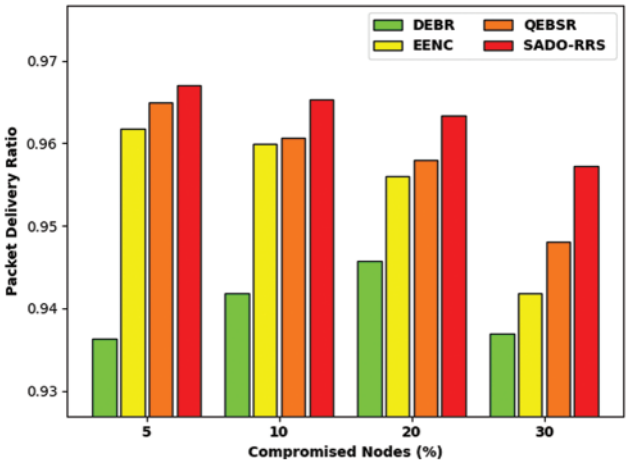

Figure 8: PDR analysis of SADO-RRS technique under distinct compromised nodes

A detailed PLR examination of the SADO-RRS technique with recent models in Tab. 5 and Fig. 9. The outcomes indicated the betterment of the SADO-RRS technique over the other methods under

distinct number of compromised nodes. For instance, with 5% of compromised nodes, the SADO-RRS technique has attained reduced PLR of 0.0330 whereas the DEBR, EENC, and QEBSR techniques have obtained least PLR of 0.0637, 0.0383, and 0.0351 respectively. Also, with 30% of compromised nodes, the SADO-RRS approach has reached lower PLR of 0.0428 whereas the DEBR, EENC, and QEBSR approaches have attained minimal PLR of 0.0631, 0.0582, and 0.0520 correspondingly.

Table 5: PLR analysis of SADO-RRS technique under distinct compromised nodes

Packet loss rate				
Compromised nodes (%)	DEBR	EENC	QEBSR	SADO-RRS
5	0.0637	0.0383	0.0351	0.0330
10	0.0582	0.0401	0.0393	0.0347
20	0.0543	0.0440	0.0420	0.0366
30	0.0631	0.0582	0.0520	0.0428

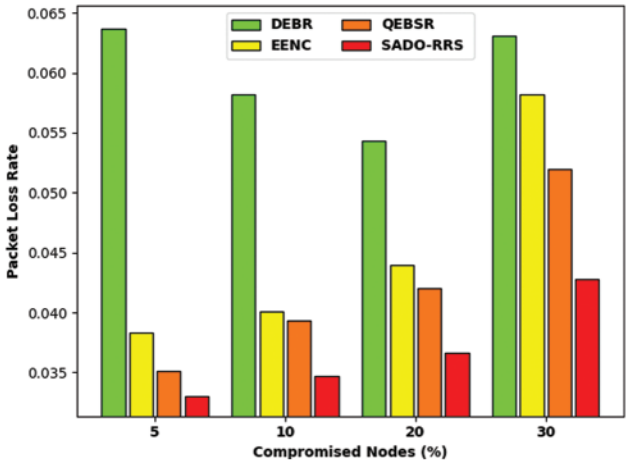

Figure 9: PLR analysis of SADO-RRS technique under distinct compromised nodes

4 Conclusion

In this study, a novel SADO-RRS technique has been developed for reliable routing in WSN. The proposed SADO-RRS technique determines the presence of attacks and optimal routes in WSN. In addition, the presented SADO-RRS technique derives a new statistics based LDA for attack detection. The presented approach develops a FF utilizing 3 input parameters such as trust level, distance to neighbors, and energy to optimum route selective. In the proposed technique, it could be vital to decrease the linear group of main functions. The experimental result analysis of the SADO-RRS technique highlighted the enhanced outcomes. In future, data aggregation approaches can be integrated into the SADO-RRS technique for enhanced performance in WSN.

Funding Statement: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia under Grant No. (KEP-81–130-42). The authors, therefore acknowledge with thanks DSR technical and financial support.

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

References

[1] H. Alwan and A. Agarwal, "Multi-objective Reliable multipath routing for wireless sensor networks," in *2010 IEEE Globecom Workshops*, Miami, FL, USA, pp. 1227–1231, 2010.

[2] M. Tariq, Y. P. Kim, J. H. Kim, Y. J. Park and E. H. Jung, "Energy efficient and reliable routing scheme for wireless sensor networks," in *2009 Int. Conf. on Communication Software and Networks*, Chengdu, China, pp. 181–185, 2009.

[3] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[4] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[5] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 59, no. 2, pp. 250–261, 2017.

[6] S. Okdem and D. Karaboga, "Routing in wireless sensor networks using ant colony optimization," in *First NASA/ESA Conf. on Adaptive Hardware and Systems (AHS'06)*, Istanbul, Turkey, pp. 401–404, 2006.

[7] K. Daabaj, M. Dixon, T. Koziniec and P. Cole, "Reliable routing scheme for indoor sensor networks," in *21st Annual IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications*, Istanbul, Turkey, pp. 1614–1619, 2010.

[8] R. Srinivasan and E. Kannan, "Energy harvesting based efficient routing scheme for wireless sensor network," *Wireless Personal Communications*, vol. 101, no. 3, pp. 1457–1468, 2018.

[9] F. Zabin, S. Misra, I. Woungang, H. F. Rashvand, N.-W. Ma *et al.,* "REEP: Data-centric, energy-efficient and reliable routing protocol for wireless sensor networks," *IET Communications*, vol. 2, no. 8, pp. 995, 2008.

[10] X. Li, W. Liu, M. Xie, A. Liu, M. Zhao *et al.,* "Differentiated data aggregation routing scheme for energy conserving and delay sensitive wireless sensor networks," *Sensors*, vol. 18, no. 7, pp. 2349, 2018.

[11] I. Banerjee, P. Chanak, H. Rahaman and T. Samanta, "Effective fault detection and routing scheme for wireless sensor networks," *Computers & Electrical Engineering*, vol. 40, no. 2, pp. 291–306, 2014.

[12] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy *et al.,* "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 170–182, 2021.

[13] K. Haseeb, A. Almogren, N. Islam, I. U. Din and Z. Jan, "An energy-efficient and secure routing protocol for intrusion avoidance in iot-based WSN," *Energies*, vol. 12, no. 21, pp. 4174, 2019.

[14] K. Haseeb, N. Islam, A. Almogren and I. Ud Din, "Intrusion prevention framework for secure routing in wsn-based mobile internet of things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[15] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah *et al.,* "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1475–1490, 2019.

[16] G. Antonogeorgos, D. Panagiotakos, K. Priftis and A. Tzonou, "Logistic regression and linear discriminant analyses in evaluating factors associated with asthma prevalence among 10- to 12-years-old children: Divergence and similarity of the two statistical methods," *International Journal of Pediatrics*, vol. 2009, no. 1, pp. 1–6, 2009.

[17] A. K. Bairwa, S. Joshi and D. Singh, "Dingo optimizer: A nature-inspired metaheuristic approach for engineering problems," *Mathematical Problems in Engineering*, vol. 2021, no. 1, pp. 1–12, 2021.
[18] J. H. A. Covarrubias, H. P. Vázquez, A. F. P. Delgado and P. M. G. Vite, "An improved dingo optimization algorithm applied to SHE-PWM modulation strategy," *Applied Sciences*, vol. 12, no. 3, pp. 992, 2022.