A Trust Aware Authentication Scheme for Wireless Sensor Networks Optimized by Salp Swarm Optimization and Deep Belief Networks

Sara A. Althubiti

Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia

Correspondence should be addressed to Sara A. Althubiti; s.althubiti@mu.edu.sa

Received 16 February 2022; Accepted 18 March 2022; Published 16 April 2022

Copyright © 2022 Sara A. Althubiti. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Presently, the integration of Internet of Things (IoT) and wireless sensor networks (WSN) offers a broad research field for enabling advanced networked services. It remains popular due to its applicability in various real-time areas such as healthcare, environmental monitoring, factory configuration, and many more. While the benefits of WSNs are many, security is still a major concern due to the intrinsic prevalence of wireless links in the network. In order to achieve security and reliable communication, an optimized authentication scheme becomes necessary. Therefore, this research work introduces a novel salp swarm optimization with deep belief network based trust aware authentication (SSDBN-TAA) scheme for WSN. Primarily, the SSDBN-TAA technique undergoes a weighted clustering scheme to partition the network into a collection of clusters. Additionally, a trust factor is collectively derived between the nodes that exist in the network, and the nodes exceeding the threshold trust value are considered as valid. An SSDBN model is utilized for dynamically selecting the threshold trust value, and the hyperparameters of the DBN model are optimally adjusted using the salp swarm algorithm (SSA). The design of SSA is efficient and thereby enhances the authentication performance. To explore the enhanced outcomes of the SSDBN-TAA technique, we conduct extensive comparative experiments to ensure the enhanced outcomes of the SSDBN-TAA system dominate the present state of art approaches.

1. Introduction

Recently, wireless sensor networks (WSN) have attracted the attention of researchers due to their dynamic nature and wide range of applications [1]. A WSN contains a tiny smart device called a micro-sensor, which has storage, constrained memory, battery resources, and processing. They utilize various types of sensors including temperature, pressure, mobility, and humidity sensors [2]. Furthermore, all sensed data is transmitted to a base station (BS) through the proper transmitting node named the cluster head (CH). As the node density and network size increase, the network scalability with data security becomes a more challenging task for WSN [3]. Lately, many solutions have been introduced for improving the energy and routing efficiency for constraint networks, but a majority of them overlook security and authentication of data in the presence of malevolent nodes. The dynamic nature of IoT systems allows a considerable amount of virtual objects and heterogeneous physical objects to be connected through the Internet [4]. The model of IoT allows these objects to interact with one another in a distributed fashion, but the transmission offers a lack of trust in data privacy [5]. Figure 1 shows the structure of IoT assisted WSN.

Traditional confidentiality resolution and safety requirements are not satisfied by operator requirements due to partial dispensation power [6]. IoT has been employed in different regions including wearable health devices observing medical grafts, conveyance supervision, distant safety control, ecological observing, and more [7]. The confidentiality and safety of information over an IoT network can be destabilized in different ways. In these contexts,
misbehaving devices may implement discriminatory attack-based trust abuse. Trust and countermeasures are a known problem domain being addressed by researchers [8]. In smart IoT, safety indications protect organizations from both risky operators and modules that might utilize the network’s vulnerabilities [9]. The safety concerns in the IoT atmosphere comprise device verification, data fortification, and admission control.

Furthermore, IoT networks must be optimized for load-balancing and energy consumption and technologically future-proofed enough to consistently route the IoT scheme for the duration of its life. In IoT environments using sensor nodes, smart inpatient systems must quickly transmit massive amounts of high-frequency information. Hence, the gateway needs to constantly authenticate the collaborating device in all the assemblies. In order to safeguard rapid authentication of devices in a legal assembly, continuous authentication is necessary. Thus, developing an intelligent and efficient IoT transmission method for ensuring data privacy with network reliability is a challenging problem [10].

The researchers in [11] present an authentication and key agreement method that allows remote users to effectively complete several authentication procedures at once from the several access conditions. This presented authentication technique is appropriate for the resource-constrained WSN structure. Cheng et al. [12] present a protocol that offers both membership authentication and key establishing concurrently to WSN. But every existing solution is only offered for either user authentication or key establishing separately. Our proposed membership authentication is complexity \(O(n)\), where \(n\) refers to the number of users from a group message, which distinguishes it from every state-of-the-art user authentication technique. The researchers in [13] present a secured and lightweighted three-factor based user verification method to WSN named SLUA-WSN. The presented method avoids privacy threat and ensures mutual authentication, anonymity, and untraceability. It can analyze the security of SLUA-WSN with informal as well as formal analyses, using automated verification of real-or-random (ROR), Burrows–Abadi–Needham (BAN) logic, and internet security protocols and applications (AVISPA).

Abdi Nasib Far et al. [14] introduce a lightweighted anonymous privacy-preserving three-factor authentication phase to WSN-related IIoT (LAPTAS). In LAPTAS, registered users utilize security smartcards for communicating with sensors and accessing their information. In contrast, our presented technique utilizes password and biometric change, revocation phase, and sensor node dynamic registration. In [15], increased symmetric key based authentication protocol to IoT based WSN is proposed. Our presented protocol is capable of countering stolen verifiers and DoS attacks while maintaining user traceability. Moreover, our presented approach simulates and verifies Proverif and BAN logic.

Furthermore, IoT networks must be enhanced for load-balancing and energy consumption systems and technologically advanced to route the IoT scheme for long life with consistent data transmission. In some IoT environments including sensor nodes, smart inpatient systems need to transmit a massive amount of information detected repeatedly to the entrance in a small time. Hence, the gateway needed to authenticate the collaborating device in all the assemblies repeatedly. In order to safeguard rapid authentication of devices in a legal assembly, continuous authentication is needed. Thus, developing an intelligent and efficient IoT transmission method for ensuring data privacy with network reliability is a difficult problem.

This paper develops a novel salp swarm optimization with deep belief network based trust aware authentication (SSDBN-TAA) scheme for WSN. The SSDBN-TAA technique applies weighted clustering scheme (WCS) for CH selection and cluster formation. In addition, we derive a trust factor between the nodes in the network. Nodes exceeding the trust value threshold are considered valid. The SSDBN model is utilized to dynamically select the threshold trust value, and the hyperparameters of the DBN model are optimally adjusted using the salp swarm algorithm (SSA). To investigate the advantages of the SSDBN-TAA technique, we make a comparison study with contemporary models.

The paper constitutes the following topics:

(i) Designing an effective SSDBN-TAA technique for accomplishing authentication in WSN
(ii) Employing a WCS for selecting CHs and constructing clusters in WSN
(iii) Deriving a trust factor for every node in the network and apply the DBN model to compute threshold trust value
(iv) Proposing an SSA technique for tuning the hyperparameter values of the DBN model
(v) Validating the effectiveness and efficiency of the SSDBN-TAA technique under a distinct number of monitoring intervals and attack frequencies

The remaining sections of this paper are organized as follows: Section 2 provides a detailed explanation of the SSDBN-TAA technique, the results of which are inspected in Section 3. Finally, Section 4 draws the key findings of the article.
2. The Proposed Model

In this study, we develop a new SSDBN-TAA system to achieve security and authentication in WSN. The proposed SSDBN-TAA technique constructs the clusters using the WCS approach. In addition, DBN based threshold value selection and SSA-based hyperparameter tuning process help to properly authenticate the nodes in WSN. When the node trust value exceeds the threshold value, it can be considered legitimate.

2.1. Weighted Clustering Scheme. The weighted clustering method determines the CH and employs cluster structure using 3 measures as node degree (ND), RE((Er)), and distance (Di). To each node, the weight \( P_i \) is calculated as follows:

\[
P_i = w_1 * RES_i + w_2 * DIS_i + w_3 * ND_i,
\]

where \( w_1, w_2 \) and \( w_3 \) represent the coefficient of model condition

\[
w_1 + w_2 + w_3 = 1.
\]

The RES of SN \((x)\) to transmit \( k \) bit data to the receiver at distance \( d \) as follows.

\[
RES = E - (E_T(k, d) + E_R(k)),
\]

where \( E \) and \( E_T \) signifies the existing energy level of SN and energy spent on data distribution.

\[
E_T(k, d) = kE_e + KE_a d^2.
\]

Here, \( E_e \) denotes electron energy and \( E_a \) indicates energy consumed for amplification.

Next, \( E_R(k) \) denotes the energy transferred on receiving data and it can be formulated as follows.

\[
E_R(k) = kE_e.
\]

Furthermore, the DIS represents the mean value of distance to adjacent nodes that exist as single-hop neighbors.

\[
DIS = \frac{\sum_{j=1}^{NB_i} dist(i, nb_j)}{NB_i},
\]

where \( dist(i, nb_j) \) designates distance of SN to the nearest \( j \) th SN.

Lastly, the NDEG represents the quantity of neighboring nodes that exist from the broadcast radius as follows.

\[
NDEG = |N(x)|.
\]

Here, \( N(x) = \{ n_y, dist(x, y) < transrange \} x \neq y \), and \( dist(x, y) \) determines the distance between two Nodes \( n_x \) and \( n_y \), \( transrange \), indicating the communication range of the Node.

2.2. Determining Trust Factor. In this phase, each node is accountable to monitor the behavior of each of its neighbors and calculates their trust value according to certain metrics.

Each trust metric has some weight that provides the capacity to adjust or control the priority of all the metrics based on the application [16, 17].

\[
DT(i, j) = \sum_{k=1}^{m} W_k * T_k(i, j),
\]

where \( m \) represent the amount of trust metrics, \( T_k(i, j) \) denotes the trust value set by node \( i \) on metric \( k \) for node \( j \); \( W_k \) indicates the weighted value of metric \( k \) thus \( \sum_{k=1}^{m} W_k = 1 \). CH estimates reliability of nodes in its cluster, and asks all the members to transmit the value they calculated about their neighbor in the similar cluster.

The CH calculates the aggregated trust value of all the nodes. Next, we calculate the overall trust value of node in its cluster by the use of following equations (9) and (10):

\[
AT(j) = \frac{1}{h} * \sum_{r=1}^{k} DT(r, j),
\]

where \( h \) indicates the amount of neighbors of node \( j \); \( DT(r, j) \) signifies the direct trust values estimated using node \( r \) for node \( j \)

\[
TT(j) = W_a * DT(CH, j) + W_b * AT(j).
\]

Here, \( W_a \) and \( W_b \) denotes weighting factor thus \( W_a + W_b = 1 \).

2.3. DBN-Based Threshold Trust Value Selection. At this stage, the DBN model has been applied to determine the threshold trust value for the authentication process. The DBN is a type of DNN with hidden layers and a massive number of hidden units. The standard DBN corresponds to the stack of RBM models with an output layer [16], as depicted in Figure 2. All the RBMs contain hidden layer \( h \) and visible layer \( v \), interconnected with undirected weights.

For the stack of RBM in the DBN, the hidden state of one RBM is considered as the visible layer of following RBM. The variable set of RBM is \( \theta = (w, b, a) \), whereas \( w_{ij} \) denotes the weight among \( v_i \) and \( h_j \). \( b_i \) and \( a_j \) indicates the bias of layer.

\[
E(\theta) = - \sum_i b_i v_i - \sum_i a_j h_j - \sum_i \sum_j w_{ij} v_i h_j,
\]

and joint likelihood distribution of \( v \) and \( h \) as

\[
p(v, h|\theta) = \frac{\exp(-E(v, h|\theta))}{\sum_{v,h} \exp(-E(v, h|\theta))}
\]

Also the marginal likelihood distribution of \( v \) as

\[
p(v|\theta) = \frac{\sum_h \exp(-E(v, h|\theta))}{\sum_v \exp(-E(v, h|\theta))}
\]

To acquire the optimum \( \theta \) for individual data vector \( v \), the gradient of log -probability evaluation is estimated by the following:
optimization approach presented by Mirjalili et al. [19]. The SSA behavior is derived by calculating it with the salp chain search for optimum food sources. In SSA, based on the individual (that is salps) position in the chain, they are separated into followers or leaders. The chain is initiated by the leader while followers obey directions for their movement.

The proposed method illustrates the pseudocode of SSA, where the similarity to another swarm intelligent algorithm and the simplicity of SSA are displayed. When it started with the salp population initialization, the swarm X of n salp is embodied as 2D matrix. Next, the salp fitness can be estimated for determining the salp using the optimal fitness (that is, leader). The leader location can be upgraded by

\[
x^l_i = \left\{ \begin{array}{ll} x^u_i & \text{if } y_i + r_1 ( (u_{ij} - l_{ij}) r_2 + l_{ij}) r_3 \geq 0, \\ x_i & \text{otherwise} \end{array} \right.
\]

(16)

Here, \( x^l_i \) represents the location of initial salp in ith parameter and \( y_i \) denotes the food location in ith parameter. \( l_{ij} \) and \( u_{ij} \) represents the lower and upper bounds of ith parameter, correspondingly, also the coefficient \( r_1 \) is estimated by the following equation. \( r_2 \) and \( r_3 \) random values within [0, 1].

\[
r_1 = 2e^{-4(L/L^2)}.
\]

(17)

Here, \( L \) represents the maximal iteration and \( l \) indicates the existing iteration. It is notable that the coefficient \( r_1 \) is significant in SSA since it balances exploration and exploitation in the whole searching method.

\[
x^j_i = \frac{1}{2} \lambda t^2 + \delta_0 t.
\]

(18)

Here, \( j \geq 2, \delta_0 \) denotes an initial speed, \( x^j_i \) represent the location of jth salp in jth dimension, \( t \) represents the time and \( \lambda = \delta_{\text{final}}/\delta_0 \) whereas \( \delta = x - x_0/\lambda t \). During optimization, the time shows the iteration. Hence, the discrepancy among iterations is equivalent to 1. Consider the assumption that \( \delta_0 = 0 \), the subsequent formula is utilized.

\[
x^j_i = \frac{1}{2} (x^j_i + x^{j-1}_i).
\]

(19)

While \( j \geq 2 \). If some salp moves outside of the searching space equation (6) demonstrates how to return them to the searching space

\[
x^j_i = \{ l \} \text{ if } x^j_i \leq l u^j i \text{ if } x^j_i \geq u^j l \text{ otherwise.}
\]

(20)

3. Experimental Validation

In this section, we perform a comprehensive result analysis of the SSDBN-TAA model under distinct metrics. Table 1 demonstrates the delay (DEL), packet delivery ratio (PDR), overhead (OH), and residual energy (RSE) examination of the SSDBN-TAA model with recent methods under distinct monitoring intervals (MIL).
Table 1: Comparison study of DBN-TAA model with existing models under several MILs.

<table>
<thead>
<tr>
<th>Monitoring interval (sec)</th>
<th>SAAC</th>
<th>SEER</th>
<th>SecLEACH</th>
<th>TMM</th>
<th>TAAPML</th>
<th>SSDBN-TAA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delay (ms)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>45.90</td>
<td>44.46</td>
<td>43.23</td>
<td>42.29</td>
<td>38.82</td>
<td>37.43</td>
</tr>
<tr>
<td>40</td>
<td>46.05</td>
<td>45.06</td>
<td>43.77</td>
<td>42.98</td>
<td>39.07</td>
<td>37.88</td>
</tr>
<tr>
<td>60</td>
<td>46.20</td>
<td>45.36</td>
<td>44.42</td>
<td>43.33</td>
<td>39.07</td>
<td>37.83</td>
</tr>
<tr>
<td>80</td>
<td>46.25</td>
<td>45.85</td>
<td>44.86</td>
<td>44.27</td>
<td>39.22</td>
<td>38.03</td>
</tr>
<tr>
<td>100</td>
<td>46.54</td>
<td>45.46</td>
<td>44.91</td>
<td>44.37</td>
<td>39.22</td>
<td>38.03</td>
</tr>
<tr>
<td><strong>Packet delivery ratio (%)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>96.12</td>
<td>96.64</td>
<td>97.07</td>
<td>97.47</td>
<td>99.07</td>
<td>99.66</td>
</tr>
<tr>
<td>40</td>
<td>96.32</td>
<td>96.84</td>
<td>97.31</td>
<td>97.85</td>
<td>99.30</td>
<td>99.75</td>
</tr>
<tr>
<td>60</td>
<td>96.73</td>
<td>97.02</td>
<td>97.60</td>
<td>98.08</td>
<td>99.57</td>
<td>99.89</td>
</tr>
<tr>
<td>80</td>
<td>96.86</td>
<td>97.22</td>
<td>97.90</td>
<td>98.49</td>
<td>99.71</td>
<td>99.95</td>
</tr>
<tr>
<td>100</td>
<td>97.04</td>
<td>97.31</td>
<td>98.17</td>
<td>99.12</td>
<td>99.98</td>
<td>99.97</td>
</tr>
<tr>
<td><strong>Residual energy (J)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>10.15</td>
<td>10.39</td>
<td>10.90</td>
<td>11.47</td>
<td>11.65</td>
<td>11.81</td>
</tr>
<tr>
<td>40</td>
<td>10.18</td>
<td>10.42</td>
<td>10.76</td>
<td>11.34</td>
<td>11.47</td>
<td>11.61</td>
</tr>
<tr>
<td>60</td>
<td>10.17</td>
<td>10.40</td>
<td>10.69</td>
<td>11.00</td>
<td>11.20</td>
<td>11.38</td>
</tr>
<tr>
<td>80</td>
<td>10.09</td>
<td>10.39</td>
<td>10.50</td>
<td>10.58</td>
<td>10.70</td>
<td>10.91</td>
</tr>
<tr>
<td>100</td>
<td>9.93</td>
<td>10.11</td>
<td>10.21</td>
<td>10.27</td>
<td>10.48</td>
<td>10.75</td>
</tr>
<tr>
<td><strong>Overhead (kb)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>527.00</td>
<td>462.00</td>
<td>325.00</td>
<td>189.00</td>
<td>157.00</td>
<td>121.00</td>
</tr>
<tr>
<td>40</td>
<td>569.00</td>
<td>514.00</td>
<td>429.00</td>
<td>390.00</td>
<td>338.00</td>
<td>254.00</td>
</tr>
<tr>
<td>60</td>
<td>650.00</td>
<td>585.00</td>
<td>510.00</td>
<td>471.00</td>
<td>416.00</td>
<td>338.00</td>
</tr>
<tr>
<td>80</td>
<td>715.00</td>
<td>650.00</td>
<td>588.00</td>
<td>559.00</td>
<td>484.00</td>
<td>413.00</td>
</tr>
<tr>
<td>100</td>
<td>803.00</td>
<td>751.00</td>
<td>705.00</td>
<td>686.00</td>
<td>621.00</td>
<td>501.00</td>
</tr>
</tbody>
</table>

Figure 3 illustrates the DEL examination of the SSDBN-TAA model with existing models under several MILs. The results indicate that the SSDBN-TAA model results in least DEL of all methods under every MIL. For instance, with an MIL of 20, the SSDBN-TAA model obtains a lower DEL of 37.43 s whereas the SAAC, SEER, SecLEACH, TMM, and TAAPML techniques result in higher DEL of 45.90 s, 44.46 s, 43.23 s, 42.29 s, and 38.82 s respectively. Along with that, with MIL of 100, the SSDBN-TAA model attains a lower DEL of 37.43 s whereas the SAAC, SEER, SecLEACH, TMM, and TAAPML techniques result in higher DEL of 45.90 s, 44.46 s, 43.23 s, 42.29 s, and 38.82 s, respectively.

A brief PDR inspection of the SSDBN-TAA model with recent approaches is provided in Figure 4. The figure reports that the SSDBN-TAA model achieves improved PDR values under every MIL. For instance, under 20 MILs, the SSDBN-TAA model reaches a higher PDR of 96.12% whereas the SAAC, SEER, SecLEACH, TMM, and TAAPML techniques achieve lower PDRs of 96.12%, 96.64%, 97.07%, 97.47%, and 99.07%, respectively. Following under 100 MILs, the SSDBN-TAA model has provided better PDR of 99.97% whereas the SAAC, SEER, SecLEACH, TMM, and TAAPML techniques have resulted in reduced PDR of 97.04%, 97.31%, 98.17%, 99.12%, and 99.98%, respectively.

Figure 5 demonstrates the OH investigation of the SSDBN-TAA model with existing models under numerous MILs. The experimental values denote that the SSDBN-TAA model achieves minimal OH over the other methods under every MIL. For instance, with an MIL of 20, the SSDBN-TAA model results in decreased OH of 121 kb whereas the SAAC, SEER, SecLEACH, TMM, and TAAPML techniques accomplish increased OH of 527 kb, 462 kb, 325 kb, 189 kb, and 157 kb respectively. Furthermore, with an MIL of 100, the SSDBN-TAA model reaches an inferior OH of 501 kb whereas the SAAC, SEER, SecLEACH, TMM, and TAAPML techniques achieve increased OH of 803 kb, 751 kb, 705 kb, and 686 kb, respectively.

A comparative RSE examination of the SSDBN-TAA model with existing techniques is provided in Figure 6. The figure states that the SSDBN-TAA model results in higher RSE values under every MIL. For instance, under 20 MILs, the SSDBN-TAA model has reached higher RSE of 11.81 J...
whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques achieve lower RSEs of 10.15 J, 10.39 J, 10.90 J, 11.47 J, and 11.65 J, respectively. Following, under 100 MILs, the SSDBN-TAA model provides a better RSE of 10.75 J whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques result in reduced RSEs of 9.93 J, 10.11 J, 10.21 J, 10.27 J, and 10.48 J, respectively.

Table 2 showcases the DEL, PDR, OH, and RSE examination of the SSDBN-TAA technique with recent approaches under various attack frequency (AF). Figure 7 depicts the DEL examination of the SSDBN-TAA system with existing methods under different AFs. The results indicate that the SSDBN-TAA model results in lower DEL over the other methods under every AF. For instance, with AF of 50 kb, the SSDBN-TAA method gains a minimum DEL of 31.27 s whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques result in higher DEL of 47.19 s, 45.52 s, 42.88 s, 38.75 s, and 36.46 s correspondingly. Likewise, with AF of 150 kb, the SSDBN-TAA algorithm has attained minimum DEL of 34.20 s whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques result in higher DEL of 47.53 s, 46.44 s, 44.43 s, 39.04 s, and 36.69 s, respectively.

A detailed PDR inspection of the SSDBN-TAA model with recent approaches is offered in Figure 8. The figure reports that the SSDBN-TAA technique achieves increased PDR values under every AF. For instance, under 50 kb AFs, the SSDBN-TAA model reaches maximum PDR of 99.08% whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML approaches achieve lower PDRs of 96.27%, 96.92%, 97.62%, 98.39%, and 98.95% correspondingly. Following, under
150 kb AFs, the SSDBN-TAA methodology provides a better PDR of 98.15% whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques result in reduced PDRs of 95.61%, 96.01%, 96.47%, 96.59%, and 97.56% correspondingly.

Figure 9 portrays the OH analysis of the SSDBN-TAA technique with existing techniques under numerous AFs. The experimental values denote that the SSDBN-TAA model achieves a minimal OH over the other methods under every AF. For instance, with AF of 50 kb, the SSDBN-TAA system results in decreased OH of 54 kb whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques achieve increased OH of 319 kb, 249 kb, 196 kb, 137 kb, and 97 kb correspondingly. Eventually, with AF of 150 kb, the SSDBN-TAA approach has reached inferior OH of 224 kb whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques have accomplished increased OH of 500 kb, 473 kb, 449 kb, 427 kb, and 227 kb, respectively.

A comparative RSE examination of the SSDBN-TAA model with existing approaches is provided in Figure 10. The figure states that the SSDBN-TAA model has resulted in...
superior RSE values under every AF. For samples under 50 kb AFs, the SSDBN-TAA approach achieves a higher RSE of 11.12 J whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques achieve lower RSEs of 10.26 J, 10.47 J, 10.66 J, 10.82 J, and 10.98 J, respectively. Finally, under 150 kb AFs, the SSDBN-TAA system has offered optimum RSE of 11.28 J whereas the SSAC, SEER, SecLEACH, TMM, and TAAPML techniques result in lower RSEs of 10.65 J, 10.89 J, 11.09 J, 11.17 J, and 11.21 J, respectively.

4. Conclusion

In this study, a new SSDBN-TAA system was developed to optimize security and authentication in WSN. The proposed SSDBN-TAA technique constructs the clusters using the WCS approach. In addition, DBN based threshold value selection and SSA based hyperparameter tuning process facilitate the proper authentication of nodes in WSN. When a node’s trust value exceeds the threshold value, it is considered legitimate. To investigate the supremacy of the SSDBN-TAA technique, we ran a series of simulations to compare them with recent models. The comparative results confirmed the enhanced outcomes of the SSDBN-TAA system over other recent state of art approaches. Therefore, the SSDBN-TAA technique can be utilized to accomplish currently-optimal secrecy in WSN. In the future, more lightweight cryptographic solutions can be designed to ensure secure communication.

Data Availability

The data are provided upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Sara A Althubiti would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2022-111.

References


