

Paper Type: Original Article

Fuzzy Trust Evaluation and Secure K-Means Clustering with Trust-Based Outlier Detection (SKC-TOD) in Wireless Sensor Networks (WSNs)

Hamiden Abd El-Wahed Khalifa^{1,*} , Amanna Ghanbari Talouki²

¹ Department of Mathematics, College of Science and Arts, Qassim University, Al-Badaya 51951 Saudi Arabia; ha.ahmed@qu.edu.sa.

² Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.

Citation:

Received: 11 March 2025
Revised: 09 April 2025
Accepted: 27 August 2025

Abd El-Wahed Khalifa, H., & Ghanbari Talouki, A. (2025). Fuzzy trust evaluation and secure K-Means clustering with trust-based outlier detection (SKC-TOD) in wireless sensor networks (WSNs). *Computational Engineering and Technology Innovations*, 2(4), 99-109.

Abstract

Secure communication and Secure Data Transmission (SDT) were considered as one of the major challenges in the Wireless Sensor Networks (WSN). Here, Fuzzy Trust Evaluation and Secure K-Means Clustering (KMC) with the Trust-based Outlier Detection (OD) Secure K-means Clustering Trust-based Outlier Detection (SKC-TOD) method was suggested in this study. The Data Transmission (DT) and evidence in Trust Values (TV) supports the Fuzzy Trust Evaluation for improving the trust of connections among the Sensor Nodes (SN). The Fuzzy C-Means (FCM) approach is used to arrange the SN into uniformly distributed clusters. This FCM method also contributes in determining the optimal Cluster Head (CH) Cluster Head Selection (CHS). The suggested SKC-TOD method was employed for enhancing accuracy. The processing time was also reduced by this suggested method. Finally, the SDT was also ensured by this suggested method. When comparing the suggested method to other current methods, the suggested method performs better than the current methods. Here, ensuring the SDT becomes a complex task for conventional methods. Then, TOD system helps in strengthening the Data Integrity (DI) against both internal and external risks. The Malicious Nodes (MN) were effectively detected and gets isolated by this TOD system. The comparative analysis was conducted among the suggested SKC-TOD and current Fuzzy clustering protocols. Form the analysis, it is clear that the suggested method is effective in enhancing SDT than the current fuzzy clustering protocols. For ensuring SDT in WSN, this suggested SKC-TOD is an effective method.

Keywords: Secure data transmission, Wireless sensor networks, K-means clustering, Outlier detection, Trust values, Fuzzy c-means, Trust-based outlier detection.

1 | Introduction

A complex challenge in many fields like environmental monitoring, business, and military applications were effectively resolved by Wireless Sensor Networks (WSN) [1]. These networks have many small, low-cost

 Corresponding Author: ha.ahmed@qu.edu.sa

 <https://doi.org/10.48314/ceti.vi.76>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

sensors with limited power and processing capabilities. These WSN networks are usually applied for wide and vulnerable settings. Data functioning and Data Integrity (DI) like selective forwarding [2], grey hole, wormhole [3], and blackhole attacks [4] were significantly impacted by several attacks because, WSN are susceptible to several attacks. The conventional methods like authentication and Secure Routing Protocols (RP) fails to detect both the internal and external attacks, because of the dynamic nature of risks [5]. The Trust Management (TM) is needed for the purpose of enhancing the performance of the network and also for improving the trust of the network. In WSN, trust means trust in the node behavior and node attributes that includes integrity and reliability. For resolving those issues, a Fuzzy Trust Evaluation with secure K-Means Clustering (KMC) and Secure K-means Clustering Trust-based Outlier Detection (SKC-TOD) was suggested in this study. This method helps in improving the Secure Data Transmission (SDT) and DI via converting data into Trust Values (TV). The Fuzzy C-Means (FCM) approach is used to arrange the Sensor Nodes (SN) into uniformly distributed clusters. The suggested method improves the Data Transmission (DT). The processing time was also reduced by this suggested method (*Fig. 1*). Finally, the SDT was also ensured by this suggested method. When comparing the suggested method to other current methods, the suggested method performs better than the current methods. However, designing SDT in WSN remains difficult because security requirements often conflict with the resource limitations of SN, such as constrained energy, memory, and computation. In addition, the network topology and traffic patterns may change over time due to node failures, mobility, or environmental conditions, which increases uncertainty in assessing node behavior. As a result, conventional security solutions and clustering protocols may exhibit higher overhead or lower detection capability when adversaries exploit internal vulnerabilities, especially in the presence of colluding or intermittently Malicious Nodes (MN). Therefore, a lightweight and adaptive mechanism that can simultaneously improve clustering stability, trust reliability, and outlier/MN identification is required to enhance network resilience and DI. To address these challenges, this study proposes the SKC-TOD framework that integrates fuzzy trust evaluation, secure clustering, and trust-based Outlier Detection (OD) into a unified process. The proposed method first converts transmission evidence and node interactions into TV and then applies fuzzy reasoning to reduce trust uncertainty and improve decision-making under ambiguous conditions. Next, the clustering procedure organizes SN into balanced clusters and supports optimal Cluster Head (CH) selection, while the trust-based OD module analyses trust deviations and behavioral inconsistencies to detect and isolate MN with higher accuracy and lower processing time. Consequently, the proposed SKC-TOD aims to enhance SDT, strengthen DI against internal/external attacks, and outperform existing fuzzy clustering-based protocols in terms of accuracy and efficiency [5].

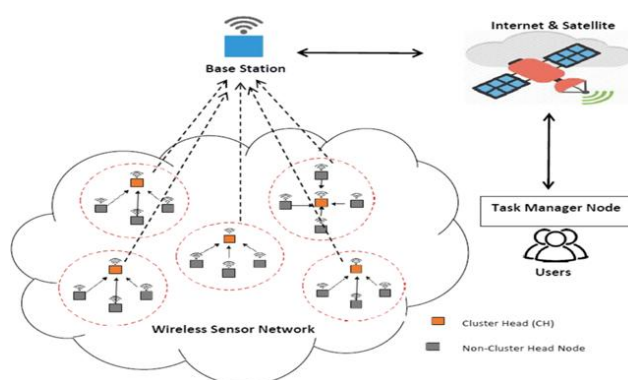


Fig. 1. Cluster-based architecture of WSN.

2 | Literature Review

Fawzy et al. [6] presented a new in-network Knowledge Discovery (KD) technique. This new in-network KD technique concurrently carried out an OD and data clustering. This approach successfully distinguished between errors resulting from environmental events and errors produced by faulty sensors. This method describes the spatial and temporal correlations among the events identified by SN in a constrained network

neighbourhood. Both real and synthetic datasets are used for the tests. The experiment's results show that the recommended approach is more efficient than the others.

In WSN, Clustering and lightweight statistical technique was employed by a method for OD, and it has been analyzed by Andrade et al. [7]. A case study using temperature sensors in WSN nodes is used to assess the methodology. The results show that even in the presence of outliers, it can generate accurate data. A Fuzzy-based Cluster Head Election (CHE) method for balancing the Energy-Efficiency (EE) and security. This method was introduced by Yang et al. [8]. The extensive tests were conducted. From the outcomes, it is clear that the network is effectively protected from intrusions by hacked nodes or internal MNs by using a secure clustering technique. This approach ensures that SN are more likely to become CH if they have higher Residual Energy (RE) or less trust in other nodes. Two density-based methods like Density-Based Spatial Clustering of Applications with Noise (DBSCAN) and Ordering Points To Identify the Clustering Structure (OPTICS) have been suggested by Abid et al. [9]. For OD and normal cluster detection, the suggested method and specific classifier is used. White Gaussian noise is introduced at various signal-to-noise ratios per data vector in order to simulate using real WSN data from the Intel Berkeley lab using MATLAB. Several input parameters and performance metrics like Detection Rate (DR) and False Alarm Rate (FAR) are used for evaluating the algorithms. When compared to current methods in WSN, the outcomes show that the DBSCAN is more accurate and comprehensive, and hierarchical dataset analysis and anomaly identification was facilitated by an effective method that is offered by OPTICS.

For WSNs, Yang et al. [10] introduced an evolutionary game-based secure clustering algorithm with fuzzy trust evaluation and OD. By transforming transmission evidence into TV, a fuzzy trust evaluation technique lowers trust uncertainty. By finding similarities and differences across SN, a K-Means-based OD technique improves the accuracy of OD by analysing more TV. The secure clustering protocol balances security and energy efficiency in CH elections. Nodes that do not become CHs can securely select their own heads, avoiding suspicious nodes. Simulations confirm that the protocol effectively defends against internal attacks and significantly improves timely data transfer rates.

A novel OD technique with a KPCA-based Mahalanobis kernel was presented by Ghorbel et al. [11]. This technique allows outliers to be distinguished from typical data patterns by implicitly mapping Data Points (DPs) in the Feature Space (FS) using the Mahalanobis distance. This approach surpasses both the original reconstruction error-based variant and the one-class Support Vector Machine (SVM) detection strategy, according to experiments conducted with real-world data from Intel Berkeley. By employing the Mahalanobis kernel, all calculations are carried out in the original space, saving processing time. Ordering Points to Identify the Clustering Structure is a density-based technique that was created by Abid et al. [12]. The suggested detector automatically configures parameters without prior environmental knowledge and extracts hierarchical clusters for post-processing classification of data into errors and events. Performance is evaluated using real and synthetic datasets from the Intel Berkeley Research lab. Results show that our method achieves an average OD rate of 81%, a precision rate of 74%, and a FAR of only 2%, which is significantly lower compared to other methods. For OD in WSN sensor data, Ahmadi Livani et al. [13] suggested a centralised method based on Principal Component Analysis (PCA) and a distributed EE method based on Distributed Clustering (DPCA). Compromised nodes or MN can produce outliers. The distributed method distributes the process among all SN and uses Fixed-Width Clustering (FWC) and DPCA for OD and create a global normal pattern. The normal profile is updated on a regular basis using weighted coefficients and a forgetting curve. The results demonstrate that the distributed strategy considerably lowers Energy Consumption (EC) and network communication overhead and achieving accuracy on par with the centralised method.

An effective cluster-based Fault Detection (FD) and recovery technique for Mobile Wireless Sensor Networks (MWSNs) was presented by Sutaone et al. [14]. The approach addresses the challenge of detecting faults and recovering from them when a CH becomes selfish or malicious. Identifying these problematic CHs is crucial, as is detecting faulty sensor data. A Trust-based Cluster head Validation and Outlier Detection Technique (TCVOD) has been suggested by researchers. In order to find and replace malicious CH, this technique first

evaluates each CH's cumulative trust. To identify and eliminate outliers in false data, the consistency of every SN is assessed. INCODE, a contextual OD framework designed specifically for WSNs, was presented by Bharti et al. [15]. To have a better understanding of DP, INCODE calculates the degree of outlierness for anomalies that are observed. Based on the concepts of Edge Computing (EC), INCODE simplifies processing and communication. Because of this, this approach is appropriate for WSNs with limited resources. The framework achieves a notable 98% accuracy in identifying outliers' contexts, while its low communication and computational demands confirm its effectiveness for environments with limited resources.

3 | Problem Statement

Problems that include secured data delivery, efficient energy, and power, then the reason for proposed methodology is to be discussed.

- I. SDT is a critical issue for WSN.
- II. Many existing protocols have tried to achieve and to enhance efficient transferring of data but none has reached its level.
- III. Many security solutions are proposed but they couldn't prevent the attacks from internally.
- IV. Many existing clustering-based protocols are tried to overcome the issue could not achieve.
- V. Proposed Secure KMC with SKC-TOD method-based Clustering Protocol is used and achieved better results in secure communication and DT.

An Interval Type-2 (IT2) Fuzzy Logic (FL)-based approach to trust evaluation is presented to convert DT, such as data tampering, data packet loss, and DT delay, into television. In addition to improving the accuracy of trust evaluation, this approach could effectively deal with the issue of trust uncertainty.

4 | Fuzzy Trust Evaluation

The IT2 FL system, renowned for its improved capacity to manage uncertainty and offer a smoother control surface, and it is discussed by researchers in this work [16]. Any Fuzzy Set (FS) in the rule base is at least one IT2 FS, which is the primary distinction of this system.

- I. Fuzzification: crisp inputs are first transformed into FS via the fuzzifier module.
- II. Inference: these FS are then processed by the inference engine in comparison to the rule base. It outlines how inputs and outputs relate to one another.
- III. Type reduction: the IT-2 FS is converted to type-1 FS using the type reduction.
- IV. Defuzzification: finally, the defuzzifier converts the fuzzy output back into a crisp value through denormalization.

To evaluate the trustworthiness of SN, we use packet dropping and delay rates as inputs to the FL system. Nine Fuzzy Rules (FR) are established to map these trust evidences to TV. For example, if both packet dropping and delay rates are low, the trust output is categorized as high trust. Let $x = (x_1, x_2)$ be the input vector for the FL system, where x_1 and x_2 denote the packet dropping rate and delay rate, respectively. To determine the output TV, the following steps should be undertaken:

- I. Using the corresponding FS of the k^{th} ($k = 1, 2, \dots, 9$) rule, $G(x_i^k)$ determine the membership grade for x_i ($i = 1, 2$).
- II. Using the product t-norm, calculate the firing grade $G(x^k)$ with respect to the k^{th} ($k = 1, 2, \dots, 9$) rule for x .
- III. Determine the output trust interval for the k^{th} ($k = 1, 2, \dots, 9$) rule for x , which is $[T_l(x^k), T_r(x^k)]$. The left TV in this case is T_l , and the right TV is T_r . In particular, the k^{th} ($k = 1, 2, \dots, 8$) rule's trust FS is

vertically symmetrical. Then, two output trust intervals are needed, one for each of the left and right parts. The firing grade should then be cut in half for any period that shares it. A Trust Set (TS) $\{< [T_l(x^t), T_r(x^t)], G(x^t) >, t = 1, 2, \dots, 16\}$ can then be obtained, which contains some value pairs of trust interval versus grade (Eq. (1)).

- IV. The TS can be reconstructed as $\{< T_a(x^t), [G_l(x^t), G_u(x^t)] >, t = 1, 2, \dots, 16\}$. by converting the value pairs of trust interval versus grade into those of TV versus grade interval. The average of the corresponding left and right TV is denoted by T_a in this case. The lower and higher membership grades of T_a with respect to the associated trust FS are G_l and G_u .
- V. Sort all of the TV in ascending order and normalise all of the lower and upper membership degrees in the trust separately. Then, $\{< T_a(x^v), [G_l(x^v), G_u(x^v)] >, v = 1, 2, \dots, 16\}$ can be used to update the TS.
- VI. Based on the TS, do type reduction using the center-of-sets approach. It is then possible to obtain a type-1 FS $1 / [T_L(x), T_R(x)]$ for the input vector x . The final left and right TV in this case are T_L and T_R , which can be defined as (Eq. (2));

$$T_L(x) = \min_{i=1,2,\dots,15} \frac{\sum_{v=1}^i G_u(x^v) \cdot T_a(x^v) + \sum_{v=i+1}^{16} G_l(x^v) \cdot T_a(x^v)}{\sum_{v=1}^i G_u(x^v) + \sum_{v=i+1}^{16} G_l(x^v)} \quad (1)$$

$$T_R(x) = \min_{j=1,2,\dots,15} \frac{\sum_{v=1}^j G_l(x^v) \cdot T_a(x^v) + \sum_{v=j+1}^{16} G_u(x^v) \cdot T_a(x^v)}{\sum_{v=1}^j G_l(x^v) + \sum_{v=j+1}^{16} G_u(x^v)} \quad (2)$$

$$= \frac{\sum_{v=1}^j G_l(x^v) \cdot T_a(x^v) + \sum_{v=j+1}^{16} G_u(x^v) \cdot T_a(x^v)}{\sum_{v=1}^j G_l(x^v) + \sum_{v=j+1}^{16} G_u(x^v)}.$$

$T_a^I < T_L < T_a^{I+1}$ is the switch point and I is on the left.

$$T_a^I, T_a^{I+1} \in \{T_a^v, v=1, 2, \dots, 16\}.$$

$T_a^J < T_R < T_a^{J+1}$ is followed by J, the right switch point.

$$T_a^J, T_a^{J+1} \in \{T_a^v, v=1, 2, \dots, 16\}.$$

Through defuzzification, the final output TV $T(x)$ for the input x can be obtained (Eq. (3)):

$$T(x) = \frac{T_L(x) + T_R(x)}{2}, \quad (3)$$

5 | Outlier Detection

Through cooperative behaviour, the SN can increase its level of trust, whether or whether it is malevolent. However, in an open wireless setting, malicious behaviour or errors in monitoring could cause its degree of trust to drop. To reliably identify whether a node is malicious, a single TV is not enough. Multiple TV collected from a node should be examined using OD techniques in order to resolve this problem. To find possible MN, a K-means based OD method is suggested in this context [17], which is carried out individually by each node. A trust recommendation mechanism is introduced to update TV more effectively and increase convergence speed. In a clustered WSN, this usually entails communication between the CH and member nodes. A node may request a trusted head for a trust recommendation when it joins the cluster. The recommended TV has been given to an SN. As shown in Eq. (4), $T(k, j)$ from CH k for node j updates the TV of node j .

$$T(i, j) = \begin{cases} \frac{T(i, j) + T(i, k)T(k, j)}{1 + T(i, k)}, & \text{if } T(i, j) > 0, \\ T(i, k)T(k, j), & \text{otherwise.} \end{cases} \quad (4)$$

The TV of nodes i through k that is updated by Fuzzy Inference (FI) is denoted by $T(i, k)$. The trust node k to j that is obtained using FI or trust recommendation is denoted by $T(i, k)$.

There are rounds to the OD process. A SN uses fuzzy clustering to update the TV of other nodes at the beginning of each round. These updated TV are then analyzed with the K-means algorithm to identify and isolate MN from potential CH. Initially, nodes do not interact, so each node records a TV of 0 for others. After interacting with more than two nodes, a node only starts its OD process. The detection procedure only proceeds in rounds when the node acts as a Cluster Member (CM) with the capacity to update TV after it has been activated.

The TS, which consists of all positive TV, is divided into two Trust Groups (TGs): the Low Trust Group (LTG) and the High Trust Group (HTG). Using the K-means algorithm, iterations allocate higher TV and lower TV to HTG and LTG in each round. The iteration process concludes when the absolute difference between the means of the two groups is less than a threshold d_m . The final means of the groups are then used as the starting points for the next round. The accumulation of trust information causes the group means to stabilise as the OD process goes on. The following are the requirements for convergence:

- I. For both TG, the absolute difference between the final group means from successive rounds is less than the d_m threshold.
- II. A threshold d_{mbg} is exceeded when the difference between the means of HTG and LTG.
- III. For T_s successive rounds, both requirements must be met.

The means of both TG tend to stabilise if the first condition is satisfied. The second condition ensures a significant difference between the groups. To prevent false positive convergence, the threshold T_s should be significantly larger than 1.

6 | Proposed Methodology

In this section [18], we introduce a detailed approach for identifying and classifying outliers in WSNs. Traditional OD techniques often overlook interesting events, while many recent methods focus solely on events and disregard erroneous data. In order to differentiate between relevant events and noisy data, researchers suggest a unique clustering-based strategy in combination with a nearest neighbor-based method for OD. The four steps of this process are as follows.

6.1 | Pre-Processing (Clustering)

An in-network clustering algorithm was initially implemented to every SN and it was facilitated by the FWC approach. With this method, every sensor reading is assigned to a cluster whose centre falls inside a specific range. If such a cluster cannot be located, a new cluster with the reading as its centre is created in the FS, providing a set of fixed-radius clusters.

6.2 | Outlier Clusters

Researchers classifies this clusters as normal or outlier clusters after generated clusters. Depending on their distance from one another, clusters are categorised as anomalies. An outlier is specifically defined as a cluster whose average Inter-Cluster (IC) distance is greater than one Standard Deviation (SD) from the mean IC distance.

Eq. (5) provides the Euclidean Distance (ED), which is employed for this measure.

$$D(x, y) = \sqrt{(x - y)^2}. \quad (5)$$

6.3 | Outlier Classification

Finding the source of outlier values is the objective of this step. To classify these values and learn more about the contributing sensors, researchers concentrate on outlier clusters. An outlier value could be the consequence of an environmental occurrence or a sensor error (such as a low battery or network damage). Usually, sensor errors are spatially correlated. However, there is probably a spatial correlation between event measurements. Both temporal and spatial correlations are common in sensor data. This is used by researchers to measure temporal correlations using timestamps and geographical correlations using data from neighboring nodes. In particular, one can identify an outlier node's neighbours. An intriguing event is indicated if these neighbor nodes generate values that are comparable to or greater than one another during the same time frame. Otherwise, the outlier value is likely erroneous. The procedure is listed below:

Step 1. To create a set of C clusters, execute the FWC algorithm.

Step 2. Determine which clusters are outliers and take the DP into account.

- I. For every cluster of outliers j :
- II. In cluster j , for every point i ,
 - Track every reading from point i th nearby nodes.
 - At point i , trace all of the readings from nearby nodes. Point i should be considered an event if these readings are equal to or larger than it and have comparable timestamps. If not, consider it an error.

6.4 | Measuring Sensor Trustworthiness

To improve the trust in classifying a sensor as reliable or error-prone, researchers calculate a trustworthiness measure for every SN after classifying outliers. The percentage of inaccurate readings from each sensor in relation to the total number of measurements is how this metric is determined.

The trustfulness measure $\text{Trust}(s_i)$ for sensor s_i is given by the Eq. (6) as follows.

$$\text{Trust}(s_i) = \left(1 - \frac{N_{oi}}{N_i}\right) \times 100. \quad (6)$$

Here, the number of incorrect readings from sensor s_i is N_{oi} . The total number of readings from sensor s_i , whether accurate or not, is N_i . They keep sensor readings over time in a temporal database or data warehouse to increase the measure's accuracy. This historical data boosts trust in the trust assessments by assisting in identifying the traits and actions of each node.

7 | Results and Discussion

In this section comparison of different current and suggested metrics and their results to be discussed. The suggested Adaptive Stochastic Gradient Descent Algorithm (ASGDA) [19]-based Clustering Protocol, integrated with SKC-TOD, performs better than the current algorithms, including the Evolutionary Game-based Secure Clustering Protocol with Fuzzy Trust Evaluation and Outlier Detection (EGSCFO) [8], Taylor Kernel FCM Clustering (TKFCC) [20], and the Secure Clustering Scheme with Cloud-based Trust Evaluation (SCCT) [21], according to Fig. 2. The SKC-TOD protocol achieves the fewest dropping attacks compared to these existing methods.

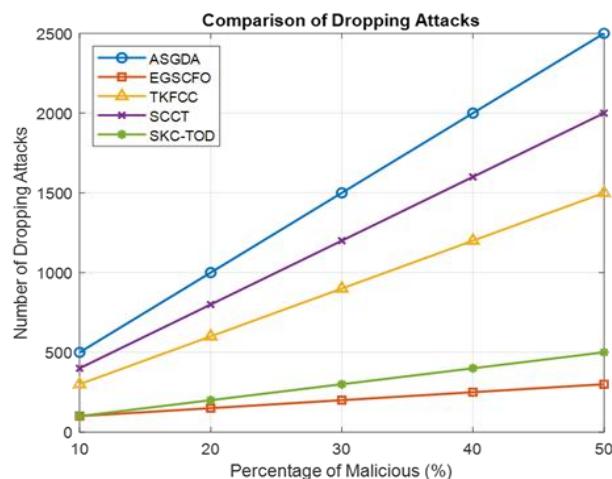


Fig. 2. The comparison of dropping attacks.

The Network Lifetime (NL) comparison of several algorithms, including the EGSCFO, TKFCC, and SCCT, is shown in Fig. 3. The suggested ASGDA-based Clustering Protocol combined with SKC-TOD is particularly noteworthy. NL is defined as the longest operational period for a given number of nodes. The results demonstrate that the ASGDA-based Clustering Protocol, combined with SKC-TOD, achieves the highest NL throughout the delivery process compared to the other methods.

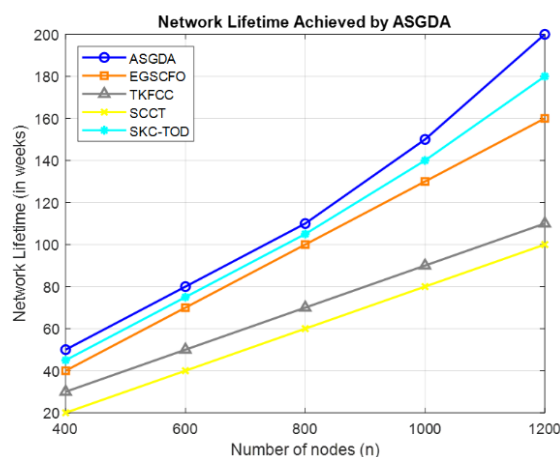


Fig. 3. NL achieved by ASGDA.

The results clearly demonstrate that SKC-TOD is enhanced by the suggested ASGDA-based Clustering Protocol. Compared to the existing methods, this current method enables a substantially lower volume of DT. The enhanced efficiency of the ASGDA algorithm ensures that more data is successfully transmitted in a timely manner, underscoring its effectiveness in optimizing data transfer within WSNs is shown in Fig. 4.

Finally, the ASGDA-based Clustering Protocol with SKC-TOD not only lowers DT efficiency but also proves to be an effective way to guarantee reliable and prompt DT in WSNs.

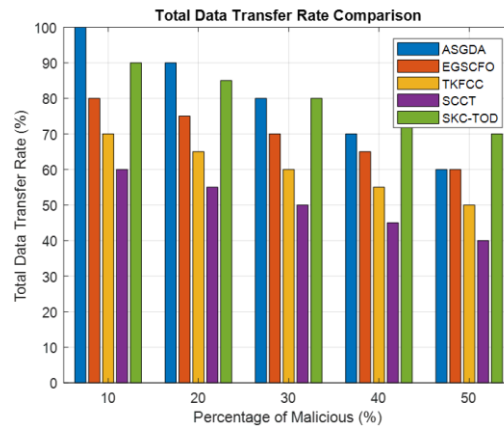


Fig. 4. The comparison of data transfer.

8 | Conclusion

The efficiency and security of DT and communication in WSN are discussed in this work. Because of the inherent shortcomings and storage capacity limitations, WSN continues to be a significant challenge. This research presents a novel method that combines the SKC-TOD protocol with Fuzzy Trust Evaluation to address these problems. By converting data and evidence into trust measures, the Fuzzy Trust Evaluation approach increases the dependability of interactions among SN. In the meantime, nodes are efficiently arranged into balanced clusters using the SKC-TOD protocol using the FCM clustering algorithm. Additionally, FCM streamlines DT procedures and improves Cluster Head Selection (CHS).

The suggested SKC-TOD method was employed for enhancing accuracy. The processing time was also reduced by this suggested method. Finally, the SDT was also ensured by this suggested method. When comparing the suggested method to other current methods, the suggested method performs better than the current methods. Here, ensuring the SDT becomes a complex task for conventional methods. Then, TOD system helps in strengthening the DI against both internal and external risks. The MN were effectively detected and gets isolated by this TOD system. The comparative analysis was conducted among the suggested SKC-TOD and current Fuzzy clustering protocols. Form the analysis, it is clear that the suggested method is effective in enhancing SDT than the current fuzzy clustering protocols. For ensuring SDT in WSN, this suggested SKC-TOD is an effective method.

Authors' Contributions

All aspects of the research and manuscript preparation were carried out by the author. The author has read and approved the final version of the manuscript.

Data Availability

All data are included in the text.

Funding

This study did not receive any specific funding from public, commercial, or non-profit funding agencies.

Conflict of Interest

The author declares that he does not have any conflict of interest.

References

- [1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE communications magazine*, 40(8), 102–114. <https://doi.org/10.1109/MCOM.2002.1024422>
- [2] Perrig, A., Szewczyk, R., Wen, V., Culler, D., & Tygar, J. (2001). SPINS: Security protocols for sensor networks. *Proceedings of the 7th annual international conference on mobile computing and networking* (pp. 189–199). Association for computing machinery. <https://doi.org/10.1145/381677.381696>
- [3] Zadeh, L. A. (1965). Fuzzy sets. *Information and control*, 8(3), 338–353. [https://doi.org/10.1016/S0019-9958\(65\)90241-X](https://doi.org/10.1016/S0019-9958(65)90241-X)
- [4] Bezdek, J. C., Ehrlich, R., & Full, W. (1984). FCM: The fuzzy c-means clustering algorithm. *Computers & geosciences*, 10(2–3), 191–203. [https://doi.org/10.1016/0098-3004\(84\)90020-7](https://doi.org/10.1016/0098-3004(84)90020-7)
- [5] Han, J., & Kamber, M. (2006). *Data mining: Concepts and techniques*. Morgan kaufmann publishers, san francisco. <https://www.amazon.com/Data-Mining-Concepts-Techniques-Management/dp/0123814790>
- [6] Fawzy, A., Mokhtar, H. M. O., & Hegazy, O. (2013). Outliers detection and classification in wireless sensor networks. *Egyptian informatics journal*, 14(2), 157–164. <https://doi.org/10.1016/j.eij.2013.06.001>
- [7] Andrade, A. T. C., Montez, C., Moraes, R., Pinto, A. R., Vasques, F., & Da Silva, G. L. (2016). Outlier detection using k-means clustering and lightweight methods for wireless sensor networks. *IECON 2016-42nd annual conference of the IEEE industrial electronics society* (pp. 4683–4688). IEEE. <https://doi.org/10.1109/IECON.2016.7794093>
- [8] Yang, L., Lu, Y., Yang, S. X., Guo, T., & Liang, Z. (2020). A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks. *IEEE transactions on industrial informatics*, 17(7), 4837–4847. <https://doi.org/10.1109/TII.2020.3019286>
- [9] Abid, A., Khediri, S. El, & Kachouri, A. (2021). Improved approaches for density-based outlier detection in wireless sensor networks. *Computing*, 103(10), 2275–2292. <https://doi.org/10.1007/s00607-021-00939-5>
- [10] Yang, L., Lu, Y., Yang, S. X., Zhong, Y., Guo, T., & Liang, Z. (2021). An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks. *IEEE sensors journal*, 21(12), 13935–13947. <https://doi.org/10.1109/JSEN.2021.3070689>
- [11] Ghorbel, O., Ayedi, W., Snoussi, H., & Abid, M. (2015). Fast and efficient outlier detection method in wireless sensor networks. *IEEE sensors journal*, 15(6), 3403–3411. <https://doi.org/10.1109/JSEN.2015.2388498>
- [12] Abid, A., Masmoudi, A., Kachouri, A., & Mahfoudhi, A. (2017). Outlier detection in wireless sensor networks based on OPTICS method for events and errors identification. *Wireless personal communications*, 97(1), 1503–1515. <https://doi.org/10.1007/s11277-017-4583-7>
- [13] Ahmadi Livani, M., Abadi, M., Alikhany, M., & Yadollahzadeh Tabari, M. (2013). Outlier detection in wireless sensor networks using distributed principal component analysis. *Journal of AI and data mining*, 1(1), 1–11. <https://doi.org/10.22044/jadm.2013.98>
- [14] Sutaone, M., Mukherj, P., & Paranjape, S. (2016). Trust-based cluster head validation and outlier detection technique for mobile wireless sensor networks. *2016 international conference on wireless communications, signal processing and networking (WiSPNET)* (pp. 2066–2070). IEEE. <https://doi.org/10.1109/WiSPNET.2016.7566505>
- [15] Bharti, S., Pattanaik, K. K., & Pandey, A. (2020). Contextual outlier detection for wireless sensor networks. *Journal of ambient intelligence and humanized computing*, 11(4), 1511–1530. <https://doi.org/10.1007/s12652-019-01194-5>
- [16] Schmidt, S., Steele, R., Dillon, T. S., & Chang, E. (2007). Fuzzy trust evaluation and credibility development in multi-agent systems. *Applied soft computing*, 7(2), 492–505. <https://doi.org/10.1016/j.asoc.2006.11.002>

- [17] Safaei, M., Asadi, S., Driss, M., Boulila, W., Alsaeedi, A., Chizari, H., ... , & Safaei, M. (2020). A systematic literature review on outlier detection in wireless sensor networks. *Symmetry*, 12(3), 1-40. <https://doi.org/10.3390/sym12030328>
- [18] Ester, M., Kriegel, H. P., Sander, J., Xu, X., ... , & Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. *Proceedings of the second international conference on knowledge discovery and data mining (KDD-96)* (pp. 226–231). Association for the advancement of artificial intelligence press. https://cdn.aaai.org/KDD/1996/KDD96-037.pdf?source=post_page-----
- [19] Verma, D., Agrawal, S., Iwendi, C., Sharma, B., Bhatia, S., & Basheer, S. (2022). A novel framework for abnormal risk classification over fetal nuchal translucency using adaptive stochastic gradient descent algorithm. *Diagnostics*, 12(11), 1-20. <https://doi.org/10.3390/diagnostics12112643>
- [20] Augustine, S., & Ananth, J. P. (2020). Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks. *Wireless networks*, 26(7), 5113–5132. <https://doi.org/10.1007/s11276-020-02352-w>
- [21] Zhang, T., Yan, L., & Yang, Y. (2018). Trust evaluation method for clustered wireless sensor networks based on cloud model. *Wireless networks*, 24(3), 777–797. <https://doi.org/10.1007/s11276-016-1368-y>