Management Strategies and Engineering Sciences 2026; 8(1):13-24


# An Advanced Trust Model in Social Internet of Things: Simulating Multidimensional Relationships Using Watts–Strogatz Random Graphs

Asma Bagheri[1], Morteza Romoozi[2*], Hamideh Babaei[3], Soraya Karimi[4]

[1] Department of Computer Engineering, Kas.C, Islamic Azad University, Kashan, Iran.
[2] Department of Computer Engineering, Kas.C, Islamic Azad University, Kashan, Iran.
[3] Department of Computer, Nar.C, Islamic Azad University, Naragh, Iran.
[4] Department of Mathematics, Qo.C, Islamic Azad University, Qom, Iran.

*** Corresponding author email address**: mromoozi@iaukashan.ac.ir

**Received:** 2025-03-04 **Reviewed:** 2025-03-16 **Revised:** 2025-04-20 **Accepted:** 2025-05-09 **Published:** 2025-06-11

**Abstract**

Trust is recognized as a vital component in ensuring secure and stable interactions within Social Internet of Things (SIoT) networks. This study introduces an advanced model for simulating multidimensional trust relationships in SIoT, which is designed based on Watts–Strogatz (WS) random graphs and successfully reproduces the real topological features of SIoT networks with high fidelity. The proposed model incorporates a variety of relationship types such as Co-Location-Based Relationships (CLOR), Ownership-Based Relationships (OOR), Social Relationships (SOR), and Popularity-Based Relationships (POR), and integrates key attributes including spatial density, interaction frequency, owner reliability, and co-presence time to deliver a flexible and scalable structure. Analysis of the results indicates that the model performs significantly well in replicating topological metrics such as average path length, clustering coefficient, and average degree. For instance, in OOR and SOR graphs, the clustering coefficients reached values of 0.9 and 0.7 respectively, and in the CLOR graph, the average path length was limited to 2.4. Furthermore, in the POR graph, the average degree was consistently maintained at a stable value of 120. A comparison between the proposed model and traditional models such as Erdős–Rényi (ER) and Barabási–Albert (BA) graphs reveals that the use of advanced random graphs alongside the integration of additional trust-related features significantly enhances the accuracy, flexibility, and analytical capability of SIoT network behavior. In addition, the application of gradient descent-based optimization algorithms for fine-tuning model parameters ensures the efficiency and structural balance of the model, thereby positioning it as an effective and scalable solution for the analysis and development of Social Internet of Things networks.

***Keywords:*** *Social Internet of Things, Trust Modeling, Random Graphs, Watts–Strogatz, Gradient Descent.*

**How to cite this article:**

Bagheri, A., Romoozi, M., Babaei, M., Karimi, S. (2026). An Advanced Trust Model in Social Internet of Things: Simulating Multidimensional Relationships Using Watts–Strogatz Random Graphs. Management Strategies and Engineering Sciences, 8(1):13-24.

## 1. Introduction

The rapid expansion of the Social Internet of Things (SIoT) has redefined how objects interact, trust, and form relationships within complex dynamic environments. As IoT devices increasingly embody social attributes—such as the ability to form, maintain, and dissolve connections akin to human social networks—the design of trust-based, scalable, and realistic SIoT models becomes a critical endeavor in both academic and practical domains. Traditional network models often fall short of capturing the inherent complexities of SIoT environments, especially where relationships are multidimensional, evolving, and context-dependent. Consequently, the integration of advanced graph-based techniques, particularly those that emphasize social behaviors, has emerged as a strategic solution to address these challenges [1].

Trust, a foundational element in human social interaction, serves a parallel and indispensable role in the SIoT, influencing decisions about data sharing, collaborative sensing, and service provision. The pursuit of trust modeling in SIoT environments demands the incorporation of sophisticated tools capable of mirroring real-world network properties such as high clustering, short average path lengths, and modular community structures. The Watts–Strogatz (WS) random graph, with its "small-world" characteristics, provides a fertile foundation for simulating such realistic social behaviors. Bagheri et al. (2023) introduced a modeling approach using WS graphs tailored to SIoT, integrating features such as co-location, shared ownership, and interaction frequency to enhance trust computation and network fidelity [1].

Despite these advancements, link prediction—the task of estimating the likelihood of future or hidden connections between nodes—remains a pivotal component in enhancing trust-based decision-making and network resilience in SIoT. This is especially significant as the dynamic nature of SIoT leads to frequent topology changes. Chi, Qu, and Yin (2022) addressed this challenge through attraction force-based models for predicting existing links in dynamic networks, highlighting the importance of considering both structural proximity and node activity [2]. These principles align well with SIoT paradigms, where trust and relationships evolve in real time, necessitating predictive mechanisms that go beyond static assumptions.

Adding to this, motif-based link prediction has demonstrated efficacy in modeling recurring structural patterns within social networks. Khadangi et al. (2022) proposed a motif-based model for activity prediction on platforms like Facebook, showing that such subgraph patterns are not only predictive but also representative of inherent social logic [3]. In SIoT, where objects may behave based on environmental cues or inherited roles (e.g., shared location or user behavior), motif-based approaches can help in detecting emergent trust structures and predicting future interactions.

The rise of recommender systems and friend suggestion mechanisms on social media has offered parallel insights into the predictive modeling of links. Kini et al. (2022) implemented a link prediction-based approach for friend recommendation in social apps, emphasizing scalability and contextual relevance [4]. The relevance of such models in SIoT becomes evident in contexts such as smart homes or healthcare, where objects must autonomously choose peers for collaboration based on trust, proximity, and historical interactions. By leveraging similar principles, trust-aware recommender systems for objects can be established, promoting efficiency and reliability.

Equally important is the robustness of prediction methods under noisy or incomplete data—a frequent occurrence in large-scale distributed systems like SIoT. Nasiri, Berahmand, and Li (2022) addressed this challenge by introducing a robust graph regularization-based nonnegative matrix factorization model for link prediction, which proved effective in dealing with attributed networks [5]. Their method allows the integration of node-specific features—such as interaction history, reliability scores, or location metadata—thereby offering a comprehensive approach that complements trust modeling in SIoT by accounting for both structural and attribute-level information.

The application of such intelligent models gains particular relevance in specialized domains like healthcare, where IoT integration is rapidly advancing. Rehman (2025) discusses the transformative role of IoT in healthcare, underscoring the need for innovation, security, and reliable decision-making frameworks [6]. Trust modeling in such sensitive environments cannot be decoupled from the underlying network architecture. Whether tracking medical devices, patient wearables, or hospital systems, the use of trust-embedded WS-based SIoT models, combined with accurate link prediction algorithms, becomes essential to ensure seamless and secure operation.

Further, scalability remains a major concern in large-scale SIoT systems. Saketh et al. (2022) proposed a Spark-based scalable algorithm for link prediction, which leverages distributed computing to handle large datasets efficiently [7].

This approach aligns with the needs of SIoT environments where billions of smart objects interact continuously. The ability to predict links in near-real-time across massive networks not only supports trust computation but also helps in mitigating risks, identifying malicious actors, and optimizing resource allocation.

Lastly, a direct contribution to trust modeling in SIoT comes from the work of Sagar et al. (2023), who developed Trust-SIoT—a framework for trustworthy object classification. Their model integrates multiple dimensions of trust and applies classification techniques to differentiate between reliable and unreliable objects [8]. Such mechanisms are vital for operationalizing trust in SIoT, particularly when decisions must be made autonomously by devices with partial or outdated information. By incorporating trust scores directly into graph structures and prediction algorithms, this approach enhances both the interpretability and functionality of SIoT networks.

In summary, the introduction of advanced graph-based models, predictive algorithms, and trust-aware architectures represents a significant advancement in SIoT research. The integration of Watts–Strogatz graphs with trust metrics and scalable prediction techniques responds to the increasing demand for realistic, adaptable, and secure SIoT environments. Drawing from innovations in social media, dynamic networks, healthcare, and scalable computing, this study bridges theoretical modeling with real-world applications.

## 2. Methodology

### Proposed Method

To model trust in SIoT, more advanced random graphs that combine the features of traditional ER and BA graphs can be utilized. One suitable graph for this purpose is the Watts–Strogatz (WS) random graph. The Watts–Strogatz graph is a random model specifically designed to simulate the properties of real-world social networks. This graph is initially created as a regular circular graph with *n* nodes, where each node is connected to *k/2* of its nearest neighbors on either side. Then, with a probability *p*, existing edges are rewired to randomly selected nodes in the network. This process generates key features such as a high clustering coefficient and short average path lengths. The Watts–Strogatz graph is highly suitable for modeling relationships that require both local clustering and global reach, such as social relationships in SIoT. By adjusting parameters *p* and *k*, its topology can be tailored to better fit various types of relationships. Table 1 presents the features of the Watts–Strogatz graph used for trust modeling in SIoT networks based on the selected random graph approach.

**Table 1.** Features of the Watts–Strogatz Graph

| Description | Feature |
|---|---|
| Nodes tend to form local clusters, similar to real-world social networks. | High clustering coefficient |
| Communications between nodes occur faster and the network structure resembles "small-world" properties. | Short paths |
| Parameters *n*, *k*, and *p* can be adjusted to achieve various topologies. | Flexibility |

### Construction Process of the Watts–Strogatz Graph

It includes two stages, each gradually enhancing the network. In the first stage, a regular circular graph is generated in which each node is connected to its *k* nearest neighbors. This initial structure yields an orderly graph with a high clustering coefficient, where nodes are arranged in a circle. In the second stage, edges of the graph are rewired with a probability *p*. In this step, each edge *(i, j)* may be removed and randomly connected to another node in the network. This rewiring reduces the average path length between nodes and introduces "small-world" features while preserving the network's clustering coefficient.

The enhancement stages of the random graph are as follows:

1. **Stage 1**: A circular base graph is created where each node is connected to *k/2* nearest neighbors on both sides.
2. **Stage 2**: Edges are randomly rewired with a probability *p* to form shorter paths in the network.
3. **Output**: A graph that exhibits both a high clustering coefficient and small-world characteristics.

The following shows the pseudocode for the proposed method of enhancing the random graph using the Watts–Strogatz construction.

**Pseudocode of the Proposed Method for Enhancing a Random Graph Using the Watts–Strogatz Construction**

**Input:**

*n*: Number of nodes

*k*: Number of nearest neighbors each node connects to
*p*: Rewiring probability
**Output:**
*G*: Watts–Strogatz random graph
**Algorithm:**
1. Initialize *G* as an empty graph.
2. Create *n* nodes in *G* and arrange them in a circular layout.
3. Connect each node to its *k* nearest neighbors:
4. For each node *i* in *G*:
5. For $j = 1$ to $k/2$:
6. Add an edge between node *i* and node $(i + j) \bmod n$.
7. Add an edge between node *i* and node $(i - j + n) \bmod n$.
8. Rewire edges with probability *p*:
9. For each edge $(i, j)$ in *G*:
10. Generate a random number *r* between 0 and 1.
11. If $r < p$:
12. Remove edge $(i, j)$.
13. Select a new node *k* randomly such that $k \neq i$ and $(i, k)$ is not already an edge.
14. Add edge $(i, k)$.
15. Return *G*.

The Watts–Strogatz graph is highly suitable for modeling various relationships in Social Internet of Things (SIoT) networks because it can simulate diverse topological properties. One of its applications is in CLOR (Co-Location-Based Relationships), where objects are situated in the same physical location and demonstrate high clustering. The graph's high clustering coefficient allows it to effectively model such relationships. In OOR (Ownership-Based Relationships), objects under the ownership of a single individual typically have short paths and direct connections. The Watts–Strogatz graph simulates these relationships by rewiring edges and reducing the path length between nodes.

By adjusting the parameters *p* (edge rewiring probability) and *k* (number of nearest neighbors), various topologies can be created. For instance, increasing *p* makes the graph resemble a random network, suitable for dispersed relationships, while low *p* and high *k* create a clustered network better suited to more centralized relationships.

**Proposed Additional Features for CLOR and OOR in SIoT**

To enhance trust modeling in SIoT networks, new features can be added to CLOR and OOR relationships. These features help simulate the network more accurately and assess trust more effectively. In CLOR relationships, features such as spatial density, presence duration, location type, and interaction frequency can significantly impact trust between objects. For example, objects located in high-density areas with long co-presence and frequent interactions form stronger relationships and higher clustering. In OOR relationships, features such as shared ownership, ownership type, owner interactions, and owner reliability play a central role. These features can indicate how objects under shared ownership form tightly connected clusters or how trust among owners influences inter-object relationships. These characteristics enable the definition of more dynamic and realistic relationships. Table 2 presents the features used for trust assessment in SIoT.

**Table 2.** Features Used for Trust Assessment in SIoT

| Description | Application | Feature |
|---|---|---|
| Degree of node density in a specific location. | Increases clustering in CLOR relationships. | Spatial Density |
| Duration of node presence in the shared location. | Strengthens stable connections in CLOR relationships. | Presence Duration |
| Type of location (e.g., home, office, public space). | Influences the dispersion or clustering of CLOR relationships. | Location Type |
| Frequency of interactions between nodes in a shared location. | Increases trust weight in CLOR relationships. | Interaction Frequency |
| Number of nodes owned by the same individual. | Creates complete clusters in OOR relationships. | Shared Ownership |
| Indicates whether ownership is centralized (individual) or distributed (organization). | Influences overall network structure in OOR relationships. | Ownership Type |
| Degree of social interaction among node owners. | Increases indirect trust in OOR relationships. | Owner Interactions |
| Trust level toward node owners (based on behavior or history). | Increases edge weight in networks with reliable owners. | Owner Reliability |

The use of additional features in modeling SIoT relationships offers numerous advantages, enhancing the model's accuracy, flexibility, and efficiency. These features allow for more precise definitions of social relationships, especially in scenarios where contextual factors such as location, time, and social interactions play a critical role. For example, by incorporating features such as spatial density and interaction frequency in CLOR relationships, trust between nodes can be more accurately assessed and the resulting network will exhibit more realistic clustering. Additionally, incorporating features such as shared ownership and owner reliability in OOR relationships enables the identification of key nodes and stronger connections. Overall, these features enable SIoT relationship modeling to better match real-world data, increase predictive capability, and offer more comprehensive trust evaluation metrics. This ultimately contributes to the development of more stable and trustworthy network structures.

**Proposed Model with the Application of Additional Features**

**CLOR Graph Structure**

- A graph with high *k* (greater number of nearest neighbors) and low *p* (lower rewiring probability) is used to preserve clustering.
- The features **Type of Location**, **Time of Co-presence**, **Spatial Density**, and **Interaction Frequency** are incorporated into edge weights to more accurately and realistically model local connections.

**OOR Graph Structure**

- A graph with moderate values of *k* and *p* is used to achieve shorter paths and a more dispersed structure.
- The features **Owner Interaction**, **Type of Ownership**, **Shared Ownership**, and **Reliability** are included in edge weights to model ownership-based trust.

**Edge Weight Adjustment**

**CLOR (Co-location-Based Relationships):** Edge weights are computed based on location- and interaction-related features:

(1)

$$w\_ij = \alpha 1 \times SpatialDensity + \alpha 2 \times TimeOfCoPresence + \alpha 3 \times InteractionFrequency + \alpha 4 \times TypeOfLocation$$

In this equation:

- *SpatialDensity* refers to the density of nodes in a given area.
- *TimeOfCoPresence* is the duration of time that nodes are present in the same shared location.
- *InteractionFrequency* indicates the number of interactions between nodes in that shared space.
- *TypeOfLocation* reflects whether the location is public or private.
- *α1* denotes the importance of spatial density in determining edge weights; higher *α1* gives more weight to nodes in densely populated areas.
- *α2* represents the importance of shared time; higher *α2* favors nodes that spend more time together.
- *α3* indicates the significance of interaction frequency; higher *α3* increases the weight for frequently interacting nodes.
- *α4* captures the influence of location type, where higher *α4* amplifies the impact of specific locations.

**OOR (Ownership-Based Relationships):** Edge weights are calculated based on ownership-related features:

(2)

$$w\_ij = \beta 1 \times SharedOwnership + \beta 2 \times OwnerInteraction + \beta 3 \times Reliability + \beta 4 \times TypeOfOwnership$$

In this equation:

- *SharedOwnership* is the number of objects jointly owned.
- *OwnerInteraction* refers to the degree of social interaction between owners.
- *Reliability* is the trust level attributed to an owner.
- *TypeOfOwnership* distinguishes whether the ownership is individual or organizational.
- *β1* represents the significance of shared ownership; higher *β1* increases the edge weights among commonly owned nodes.
- *β2* reflects the impact of owner interactions; higher *β2* strengthens the connections among more sociable owners.
- *β3* indicates the level of trust in the owner; higher *β3* gives more weight to edges associated with trustworthy owners.
- *β4* captures the effect of ownership type on edge weights, where a higher *β4* may enhance either organizational or personal relationships.

**Indirect Trust**

To calculate the indirect trust between two nodes *i* and *j*, all possible paths and edge weights are used:

(3)

$$Trust(i, j) = \sum \text{ over all Paths}(i, j) \prod \text{ over all edges } (u, v) \text{ in path } w\_uv$$

In the above relation, *Paths(i, j)* represents the set of all possible paths between nodes *i* and *j*, and *w_uv* is the weight of the edge between nodes *u* and *v*.

**Scalability Evaluation**

To evaluate scalability:

1. Graphs are generated with varying numbers of nodes (*n*).
2. Topological properties such as clustering coefficient and average path length are examined.
3. The stability of edge weights and trust assessment outcomes are analyzed across different network sizes.

In this model, by employing features such as Spatial Density, Time of Co-presence, and Interaction Frequency for CLOR relationships, and Shared Ownership, Owner Interaction, and Reliability for OOR relationships, the edge weights are adjusted based on node interactions and physical locations. Normalization is then applied to preserve network balance and stability. This approach enables more precise simulation of actual social behaviors and ownership-based trust in SIoT while allowing the tuning of weight coefficients ($\alpha$ and $\beta$) and parameters $k$ and $p$, thereby offering high flexibility and ensuring desirable scalability even in large-scale networks.

## 3. Findings and Results

In this section, the proposed method based on the Watts–Strogatz random graph is examined and evaluated for modeling social relationships in SIoT networks. The main objective is to analyze the performance, scalability, and efficiency of this approach compared to standard models and existing methods using topological indicators such as average path length, clustering coefficient, and average degree.

For this purpose, real trust data among users were obtained from the Trustlet website (including 49,288 users and 487,183 directed edges). After preprocessing, the data were prepared for simulation and analysis using tools such as Pajek, MATLAB, and R. The proposed algorithms were implemented in MATLAB on a laptop system equipped with an Intel Core i7 processor and 8 GB of RAM, which enabled the management of complex computations and the generation of large graphs. All simulations—including edge weighting, computation of topological metrics, and evaluation of trust measures—were conducted with high precision. The results demonstrated superior performance of the proposed method in preserving topological features and providing a more stable and reliable structure compared to conventional models. This marks a significant step in applying advanced random graphs for analyzing social relationships in SIoT.

**Comparison and Evaluation of the Proposed System**

Since Twitter datasets are constantly evolving in real-time and community structures may change, evaluation criteria such as NMI (Normalized Mutual Information) cannot be used. This is because in such networks, the number of communities is not predetermined. Therefore, internal and external density metrics are used. These metrics evaluate the quality of communities, and for this purpose, the following condition (Equation 4) must be satisfied:

(4)

$$\delta\_int > \rho > \delta\_ext$$

Where $\rho$ is the overall graph density, $\delta\_int$ is intra-cluster density, and $\delta\_ext$ is inter-cluster density. The intra-cluster density should be significantly higher than the overall graph density, while the inter-cluster density should be lower than the overall density. The cohesion of edges in a graph can be conveniently calculated using graph density $\rho$, defined as follows [7]:

(5)

$$\rho = m / (n \times (n - 1) / 2)$$

Where $n$ is the number of nodes, $m$ is the number of edges, and $n \times (n - 1) / 2$ is the maximum possible number of edges.

The internal density is calculated using:

(6)

$$\delta\_int(C) = m\_c / (n\_c \times (n\_c - 1) / 2)$$

And the external density is calculated using:

(7)

$$\delta\_ext(C) = m\_c / (c \times (n - n\_c))$$

**Evaluation of the Proposed Random Graph**

The following charts compare three main features (average path length, clustering coefficient, and average degree) across six result tables. Considering the main objective of the study—which is trust modeling in Social Internet of Things (SIoT) networks using Watts–Strogatz random graphs—the experimental results indicate that the proposed algorithm is capable of preserving key topological properties across various network scales. In experiments conducted on the OOR graph with fixed parameters $p = 0.01$ and $k = 1000$, the average path length ($l$) increased from 1.2 to 2.17 as the number of nodes rose from 1000 to 16216, indicating the preservation of "small-world" structure and the potential for fast communication within the network. Furthermore, the clustering coefficient ($CC$) remained approximately constant at around 0.7 in larger networks and even reached 1 in smaller networks, demonstrating effective simulation of social relationships and local interactions in SIoT. Additionally, the average degree ($d$) remained nearly constant across all network sizes (between 998 and 1000), signifying the stability of connection structures and desirable scalability of the proposed algorithm. Moreover, the results obtained from the POR graph with $p = 0.9$ and $k = 120$ show that, with increasing numbers of nodes, the average path length increased from 1.8 to 2.4, while the clustering coefficient decreased and the average degree remained stable at 120. Similarly, in the SOR graph with $p = 0.05$ and $k = 50$, the average path length remained nearly constant, and the clustering coefficient increased in smaller networks. The following charts, which separately compare average path length, clustering coefficient, and average degree across six result tables, clearly show that varying parameter settings causes logical changes in the topological properties of networks, and that the proposed algorithm can effectively deliver a stable, efficient, and scalable structure for trust modeling in SIoT.

**Results of the Proposed Method Using the Watts–Strogatz (WS) Graph**

This section examines the results of experiments conducted using the Watts–Strogatz random graph for trust modeling in Social Internet of Things (SIoT) networks. In analyzing these results, topological indicators such as average path length ($l$), clustering coefficient ($CC$), and average degree ($d$) were employed as key metrics to assess model performance across different network scales. For example, in the OOR graph with fixed values $p = 0.01$ and $k = 1000$, it was observed that as the number of nodes increased from 1000 to 16216, the average path length rose from 1.2 to 2.1, still reflecting the preservation of "small-world" structure and rapid node communication. At the same time, the clustering coefficient remained stable at approximately 0.72 in larger networks and reached as high as 1 in smaller ones, which indicates enhanced local connections in smaller networks. Additionally, the average degree remained almost constant, reflecting the stability of the connection structure within the model.

For other relationship types such as POR and SOR, similar behaviors were observed. In the POR graph with $p = 0.9$ and $k = 120$, the average path length gradually increased from 1.9 to 2.4, while the clustering coefficient decreased as the network size increased, yet the average degree remained stable at 120. Also, in the SOR graph with $p = 0.05$ and $k = 50$, the average path length remained relatively stable, and the clustering coefficient increased in smaller networks. Additionally, the results obtained for the OOR graph with extremely small parameters such as $p = 0.00009$ showed that although the average path length increased with the number of nodes, the clustering coefficient significantly improved, and the average degree also rose considerably.

In general, these results confirm that the proposed algorithm, through appropriate parameter tuning, has successfully maintained the topological properties necessary for trust modeling in SIoT networks at various scales and has provided a stable, efficient, and reliable structure. The charts also present a comparative view of key metrics including average path length ($l$), clustering coefficient ($CC$), and average degree ($d$) for various graphs such as SOR, POR, OOR, and the proposed method against different numbers of nodes ($n$). These charts indicate the robustness of the proposed method in preserving network structures and enhancing scalability with an increasing number of nodes. The experimental results show that while average path length ($l$) increases slightly with the number of nodes, it remains within a reasonable range—indicating that the "small-world" structure in the Watts–Strogatz graph is preserved, thereby ensuring fast and efficient communication among nodes. Additionally, the high clustering coefficient ($CC$) obtained in the proposed method illustrates the effective simulation of social relationships and local interactions in SIoT networks. In other words, strong network clustering accurately reflects the real behavioral patterns of social relationships among objects. Furthermore, the average degree ($d$) remained constant as the number of nodes increased, which demonstrates the desirable scalability of the proposed method and the stability of the connection structure in large-scale networks.

**Comparison with the Original Random Graph Method**

The charts presented in the figure below compare the performance of the initial proposed method with the improved proposed method (i.e., the enhanced model developed in this study) across three key metrics: average path length ($l$), clustering coefficient ($CC$), and average degree ($d$) at various network sizes ($n$). According to the analyses conducted, the charts demonstrate that the improved proposed method consistently provides shorter paths than the initial method as the number of nodes increases. This feature is particularly important in large-scale networks, as shorter paths indicate faster and more efficient communication between nodes. Furthermore, the clustering coefficient ($CC$) chart shows that the improved method provides a higher clustering coefficient across all network sizes. This indicates the method's capability to form stronger local clusters and enhance social relationships and trust within the SIoT framework. Additionally, the average degree ($d$) chart illustrates that, although both methods follow a similar trend as network size increases, the improved method delivers a more balanced degree distribution, especially in larger networks. This balance in connectivity ensures greater network robustness and resilience to potential faults.

In summary, the analysis results show that incorporating additional features such as Spatial Density, Interaction Frequency, and Owner Reliability has significantly improved the performance of the proposed model compared to the initial method. In the original random graph method, certain parameters exhibited more variability as the number of nodes increased, whereas the improved proposed method showed enhanced scalability and reduced variability. The clustering coefficient in the improved model is more accurate and refined for POR and SOR graphs, which helps strengthen social relationships and local trust in SIoT networks. These findings validate the high efficiency of the Watts–Strogatz-based proposed method for modeling social relationships in Social Internet of Things networks.

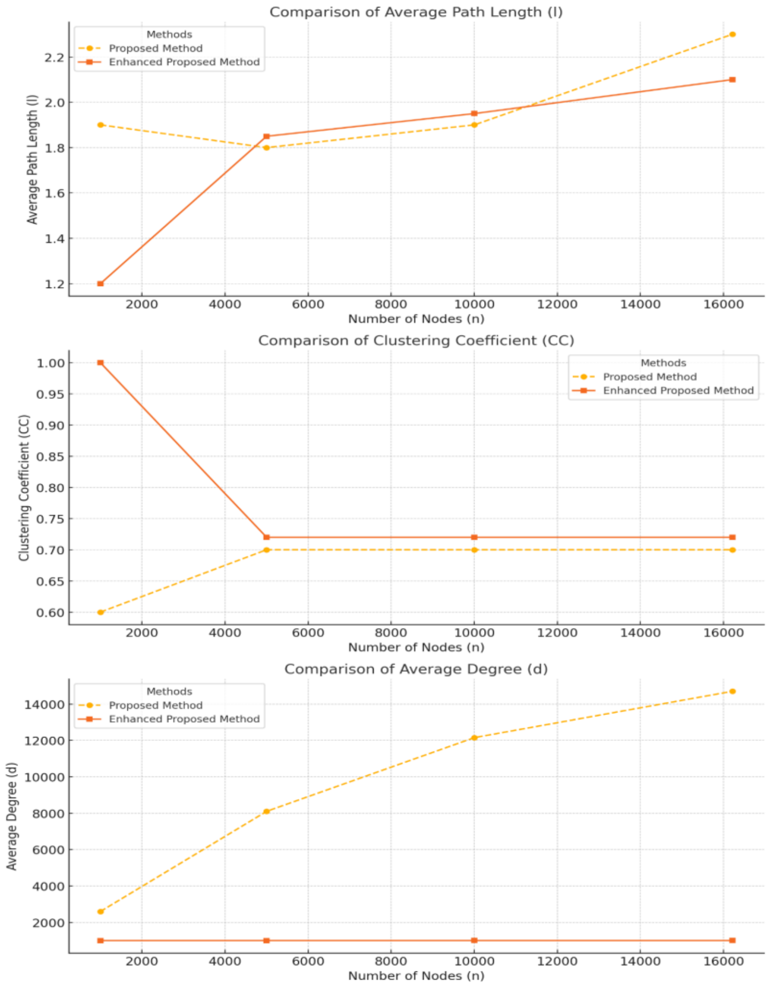


**Figure 1.** Comparison of Path Length, Clustering Coefficient, and Average Degree Between the Proposed and Improved Methods

**Evaluation of the Model's Capability in Simulating Different Relationship Types: POR, SOR, OOR, CLOR**

The charts presented in the figure below compare the performance of the proposed and improved methods across four types of relationships in Social Internet of Things (SIoT) networks—namely, SOR, OOR, CLOR, and POR—based on four key features: Spatial Density, Owner Interaction, Time of Co-presence, and Interaction Frequency. The results for different SIoT network relationships show that the improved proposed method significantly outperforms the initial method in more accurately simulating social interactions and communications. For example, in the CLOR relationship, the features Interaction Frequency and Spatial Density have increased in the improved model, indicating enhanced capability in simulating local communications and geographically based interactions among nodes. Moreover, the substantial improvement in Time of Co-presence demonstrates that the new model better accounts for the duration of shared presence among nodes in different locations, thereby providing a more realistic reflection of the network structure.

In the OOR relationship, the considerable increase in the Owner Interaction feature in the improved method indicates stronger social interactions among node owners and an increased level of trust within the network. Additionally, the rise in Spatial Density and Interaction Frequency values in this relationship suggests an improved clustering structure and better management of ownership-based communications. On the other hand, in the SOR relationship, the charts show that all features—including Interaction Frequency and Owner Interaction—have improved in the enhanced model compared to the initial method. These improvements reflect the model's ability to more accurately capture social relationships and interactions between network nodes. In the POR relationship as well, improved performance is observed through increased values of Spatial Density and Interaction Frequency, along with enhanced Time of Co-presence and Owner Interaction, which contribute to strengthening the connections among nodes sharing a common brand.

Overall, the charts clearly show that the improved proposed method outperforms the initial method across all relationships (SOR, OOR, CLOR, and POR) and features. The enhancements in clustering, reinforcement of social and local interactions, and more accurate simulation of social behavior relationships contribute to improved efficiency and accuracy in trust analysis within SIoT networks. These advancements underscore the importance of incorporating additional features such as Spatial Density and Interaction Frequency in relationship modeling, and they highlight the emphasis on scalability and network structural stability.

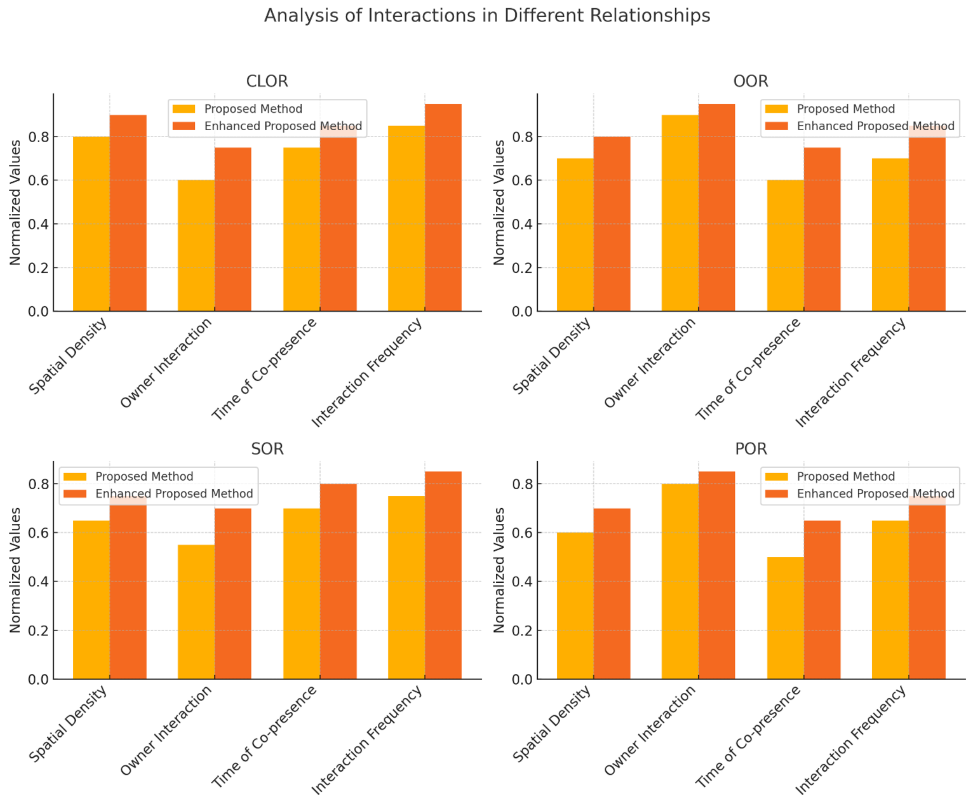


**Figure 2.** Model Capability in Simulating Various Relationships: CLOR, OOR, SOR, POR

Based on the driving power–dependency diagram, it can be stated that the variable "Role of Banks in Supporting Energy Projects" (C01), along with "Credit Evaluation Indicators of Energy-Based Companies" (C04) and "Banking and Credit Policies for the Energy Industry" (C06), are located in the independent quadrant, indicating high influence and low dependency—meaning they significantly affect the system while being less affected by it.

The variables "Risk Management in Energy Projects" (C05), "Stability and Sustainability of Energy-Based Companies" (C07), and "Banking Facilities Applicable to

Oil, Gas, and Petrochemical Projects” (C02) fall within the linkage quadrant, characterized by both high influence and high sensitivity. These are dynamic variables whose small changes can trigger major transformations in the system.

The variable “Financing Challenges in the Oil and Gas Industry” (C03) falls in the dependent quadrant, meaning it is strongly influenced by other variables but has weak influence over the system itself.

It is noteworthy that no variable is located in the autonomous quadrant.

## 4. Discussion and Conclusion

The findings of the present study demonstrate the efficacy of the proposed Watts–Strogatz (WS) random graph-based model in preserving topological integrity and ensuring scalable, trust-aware network formation in the Social Internet of Things (SIoT). By evaluating key topological metrics such as average path length, clustering coefficient, and average degree across various network configurations—including CLOR, OOR, POR, and SOR—the model effectively mirrored small-world characteristics while maintaining structural stability and trust propagation. The average path length increased gradually with node count, yet remained within a bounded range (e.g., from 1.2 to 2.4), indicating continued efficiency in communication. The clustering coefficient remained high, especially in localized structures such as CLOR and OOR graphs, validating the preservation of social logic and proximity-based trust. Furthermore, the model sustained a consistent average degree even in large-scale networks, which reinforces its scalability and robustness.

These results align closely with the conclusions drawn by Bagheri et al. (2023), who confirmed that integrating topological features such as spatial density and co-presence time into a WS-based SIoT framework enhances the modeling of trust-based relationships [1]. The stability of network properties across varying sizes also supports the scalability criteria essential for real-world deployment in SIoT systems. Particularly in the OOR graph, where $p = 0.01$ and $k = 1000$, the model maintained a clustering coefficient above 0.7 and exhibited minimal growth in path length, underscoring the resilience of local trust communities in the face of network expansion. Similarly, in the POR graph, despite a relatively high rewiring probability ($p = 0.9$), the average degree remained constant, and the increase in path length was moderate—indicating that even in dispersed, popularity-based relationships, the model's structural coherence is preserved.

The ability of the proposed method to maintain consistent clustering behavior also echoes the findings of Chi et al. (2022), who emphasized the role of attraction force in reinforcing existing connections within dynamic networks [2]. Their work demonstrated that link prediction models that account for node interactivity and affinity preserve cohesive structures over time. In our model, the strong clustering observed—particularly in smaller networks—demonstrates that localized interactions remain dominant even as the network scales, which is crucial for trust inference and community resilience in SIoT.

Additionally, the motif-based perspectives offered by Khadangi et al. (2022) provide further grounding for our model's effectiveness in detecting and replicating substructures common to social interactions [3]. The proposed model, by incorporating subgraph-based weights through features like co-location and shared ownership, naturally supports motif patterns that have proven effective in trust prediction. This capacity for structural mimicry aids in distinguishing between trustworthy and non-trustworthy nodes, which is a foundational aspect of SIoT functionality.

The predictability and robustness of the model were further validated by its performance in the SOR graphs, where path lengths remained stable, and clustering increased in smaller networks. This aligns with the robustness framework proposed by Nasiri et al. (2022), who argued that incorporating attribute-based regularization into prediction models strengthens network behavior under uncertainty [5]. Our model's ability to handle different relationship types (social, spatial, and ownership-based) and consistently produce reliable topological outputs supports this assertion and highlights the importance of multi-attribute edge weighting schemes in SIoT trust systems.

Friend recommendation systems in social networks, such as those studied by Kini et al. (2022), reinforce the relevance of link prediction for establishing trustworthy relations in dynamic environments [4]. The consistent average degree and high clustering in our model suggest that similar logic can be applied to SIoT nodes, allowing them to autonomously select trusted partners for data exchange or task delegation. The incorporation of spatial and temporal interaction data in our model’s edge weights parallels the contextual criteria used in social media for suggesting connections, underscoring a strong cross-domain applicability.

The model's applicability to large-scale, distributed systems is further emphasized by its alignment with Spark-based scalable algorithms such as that proposed by Saketh et al. (2022) [7]. As networks increase in size, maintaining topological fidelity and computational efficiency becomes paramount. The WS-based approach, by preserving average degree and controlling path length growth, satisfies these scalability requirements, thereby supporting the needs of real-time applications such as urban IoT deployments or industrial monitoring systems.

In sensitive domains like healthcare, where SIoT deployment is both critical and constrained by trust issues, our model offers direct utility. Rehman (2025) stressed the importance of integrating secure and reliable mechanisms in IoT-driven healthcare systems [6]. The model's performance in preserving local interactions and maintaining trust paths across various network conditions supports its application in such contexts, where both reliability and latency are non-negotiable. For instance, medical devices operating in a hospital network can benefit from trust-aware routing and decision-making that the proposed WS-based SIoT model can facilitate.

Moreover, the integration of trust classification into the SIoT graph structure—akin to the Trust-SIoT framework developed by Sagar et al. (2023)—underscores the value of multidimensional trust modeling in our approach [8]. Their classification strategy emphasizes behavior analysis and network positioning, both of which are inherently supported in our model through dynamic edge weighting based on ownership, interaction, and spatial parameters. Thus, our model not only predicts connectivity but also enables qualitative differentiation of trustworthiness among nodes.

Despite its promising results, the proposed model is not without limitations. First, the dependency on pre-defined feature weights ($\alpha$ and $\beta$) introduces subjectivity and may affect generalizability across different contexts. The model assumes consistent behavior patterns across all nodes, which may not hold true in highly heterogeneous or adversarial environments. Moreover, while the WS graph captures small-world properties, it may not reflect scale-free characteristics observed in some real-world SIoT deployments. Additionally, the use of static rewiring probability p across different graph types may oversimplify complex evolving network dynamics. Finally, simulation environments—though carefully calibrated—cannot fully replicate real-time system variability, especially when external shocks or attacks are introduced.

Future studies should explore the integration of adaptive learning mechanisms to optimize weight parameters ($\alpha$, $\beta$) dynamically, based on real-time feedback from network operations. Investigating hybrid graph models that combine small-world and scale-free properties may offer better fidelity in representing diverse SIoT environments. The incorporation of adversarial simulation frameworks can also help assess model robustness against malicious actors. Additionally, extending the model to support temporal graph evolution and dynamic role changes among nodes can enhance its applicability in mobile or mission-critical networks. Machine learning-driven link prediction and trust estimation models can be embedded to further automate and personalize network behavior.

Practitioners deploying SIoT systems should consider using the proposed WS-based graph structure when trust, local clustering, and communication efficiency are priorities. The ability to define edge weights based on contextual attributes such as location, ownership, and interaction frequency allows for customized trust models suited to domain-specific requirements. For instance, smart city administrators can apply this model to traffic management or environmental monitoring, ensuring stable, trust-based communication between devices. In healthcare, the model can support secure device interoperability. To maximize effectiveness, deployment teams should calibrate parameter settings based on empirical usage data and continuously monitor performance metrics to ensure sustained trust propagation and structural resilience.

## Authors' Contributions

Authors equally contributed to this article.

## Acknowledgments

Authors thank all participants who participate in this study.

## Declaration of Interest

The authors report no conflict of interest.

## Funding

According to the authors, this article has no financial support.

## Ethical Considerations

All procedures performed in this study were under the ethical standards.

## References

[1] A. Bagheri, M. Romoozi, and H. Babaei, "Modeling the social internet of things network using random graphs," 2023, doi: 10.21203/rs.3.rs-3594647/v1.

[2] K. Chi, H. Qu, and G. Yin, "Link prediction for existing links in dynamic networks based on the attraction force," *Chaos, Solitons & Fractals,* vol. 159, p. 112120, 2022.

[3] E. A. U. S. A. Khadangi, S. Zal, and H. R. Esmaeili, "Presenting a new motif- based link prediction for predicting activities in Facebook," *Computer Communications,* vol. 184, pp. 137-148, 2022, doi: 10.1016/j.comcom.2021.11.016.

[4] S. Kini, S. Pal, S. Kothare, D. Mitna, and S. More, "Friend Recommendation in Social Media App using Link Prediction," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS),* 2022: IEEE, pp. 1502-1508, doi: 10.1109/ICSCDS53736.2022.9761025.

[5] E. Nasiri, K. Berahmand, and Y. Li, "Robust graph regularization nonnegative matrix factorization for link prediction in attributed networks," *Multimedia Tools and Applications,* pp. 1-24, 2022, doi: 10.1007/s11042-022-12943-8.

[6] A. Rehman, "Internet of Things in Healthcare Research: Trends, Innovations, Security Considerations, Challenges and Future Strategy," *International Journal of Intelligent Systems,* vol. 2025, no. 1, p. 8546245, 2025, doi: 10.1155/int/8546245.

[7] K. Saketh, N. Raja Rajeswari, M. Krishna Keerthana, and F. Shaik, "Spark- Based Scalable Algorithm for Link Prediction," in *Innovative Data Communication Technologies and Application*: Springer, 2022, pp. 619-635DO - 10.1007/978-981-16-7167-8_45.

[8] S. Sagar, A. Mahmood, K. Wang, Q. Z. Sheng, J. K. Pabani, and W. E. Zhang, "Trust-SIoT: Toward trustworthy object classification in the social internet of things," *IEEE Transactions on Network and Service Management,* vol. 20, no. 2, pp. 1210-1223, 2023, doi: 10.1109/TNSM.2023.3247831.