Markov Chain-Based Analytical Model Supporting Service Provisioning and Network Design in the Social Internet of Everything

Giancarlo Sciddurlo[a,b], Pietro Camarda[a], Domenico Striccoli[a], Ilaria Cianci[a], Giuseppe Piro[a,b], Gennaro Boggia[a,b]

[a] *Department of Electrical and Information Engineering, Politecnico di Bari, Bari, Italy*
[b] *CNIT, Consorzio Nazionale Interuniversitario per le Telecomunicazioni*

Abstract

The Internet of Everything has emerged as a prominent paradigm, enabling the development of advanced services by integrating smart objects, individuals, processes, and data. In the context of social networking within this framework, addressing the inherent uncertainty of the environment and developing secure service provisioning mechanisms is crucial. At present, there has been limited exploration into the stochastic behavior of the service fulfillment process, especially when considering the trustworthiness and resource availability of service providers. Additionally, existing approaches supporting service provisioning often require continuous and computationally prohibitive efforts. To overcome these challenges, this paper introduces a Markov chain-based stochastic model that effectively predicts the steady-state behavior of service providers within an IoE network. The proposed model integrates both the trust levels and resource capabilities of providers to ensure successful service delivery, while simultaneously identifying and excluding malicious entities without imposing significant computational overhead. The validity of the model is demonstrated by comparing various performance metrics against results obtained from extensive simulations, highlighting its effectiveness and practical applicability. Ultimately, the model serves as a valuable tool for fostering trusted service provisioning, optimizing the design of service communities within social networks, preventing data traffic loss, and enhancing the overall reliability and responsiveness of the system.

Keywords: Social Internet of Everything, Markov Chain Model, Trust Management System, Service Provisioning

1. Introduction

The Internet of Everything (IoE) expands upon the concept of the Internet of Things (IoT) by integrating interconnected smart objects, individuals, processes, and data, creating new opportunities and unlocking substantial economic potential [1]. Furthermore, it is distinguished by complex interconnections and interactions involving a wide range of technologies, devices, and stakeholders [2].

Within this framework, social networking presents a valuable solution by facilitating collaboration and interaction among entities, thereby enhancing resource sharing and enabling efficient service provisioning [3, 4].The integration of social networking capabilities into the IoE introduces the concept of the Social Internet of Everything (SIoE), which has significant potential to impact various domains, such as healthcare [5], the Internet of Vehicles [6, 7], and smart cities [8, 9]. Furthermore, the incorporation of social skills enables access to information and services from anywhere at any time, enhancing network resource visibility and facilitating efficient service discovery [10]. Consequently, representing social linkages within a virtual environment not only improves network scalability and navigability but also allows for the assessment of stakeholders' reputations, ultimately leading to more reliable service provisioning [11].

However, the pervasiveness of devices within the most intimate aspects of individuals' lives presents complex challenges for researchers to address [12]. The prompt and successful completion of services is significantly influenced by the availability of service providers and their limited resources. Moreover, selecting the most appropriate service provider requires careful consideration of their trustworthiness, which involves multiple interrelated factors, such as the provider's social ties with other entities [13] and their reputation based on previous interactions [14]. Complicating matters further is the inherently stochastic nature of SIoE systems. Accurately modeling this unpredictable behavior is essential for evaluating the process of selecting a trusted service provider.

It is worth noting that numerous studies in the literature address trust management in the service provisioning process within the context of Social Networks and the IoE [14–24]. However, to the best of the authors' knowledge, existing models typically necessitate time-continuous and computationally intensive efforts to monitor the long-term evolution of the service provisioning process. This includes maintaining a record of social-based interactions and estimating the trust levels of service providers, which can be computationally prohibitive [16]. Additionally, some models struggle to manage high-volume traffic effectively [25]. Furthermore, none of the trust-based models in the literature explicitly consider the resource availability of the entities involved in the service provisioning process.

In addressing these open issues, this work aims to extend and enhance the existing scientific literature. The main contributions of this study are summarized as follows:

1. A stochastic analytical model, based on a multidimensional Markov chain, is developed to capture the state of a generic service provider. Specifically, the model predicts the steady-state reputational behavior of an SIoE entity by simultaneously considering multiple factors, including friendship relationships, trust levels, and the available resources of service providers.
2. The proposed strategy is capable of tracking the evolution of each SIoE entity's reputation, thereby assessing the overall capability of the SIoE network to successfully fulfill services. It also identifies and excludes malicious nodes from the provider selection process, ensuring system reliability. Notably, this objective is achieved without requiring extensive computational resources improving practicality, efficiency, and responsiveness. As a result, the model is highly suitable for real-world applications and environments.
3. The analytical model is validated through a comparative analysis of various performance metrics against results obtained from extensive simulations, demonstrating its effectiveness and applicability in complex SIoE scenarios.
4. Finally, by evaluating available resources, the proposed model is employed to optimally design the SIoE environment, ensuring it can support various request loads in a reliable and responsive manner. Furthermore, due to its capability to identify entities with malicious intent, it is utilized as a tool for investigating specific and well-documented reliability attacks in service network provisioning.

The remainder of this paper is organized as follows: Section 2 reviews related works, outlines the objectives of this contribution, and presents the SIoE reference scenario. Section 3 formulates the novel Markov chain model designed to evaluate the behavior of an entity within a SIoE environment. Section 4 discusses insights derived from the model's outcomes. Model validation and experimental results are detailed in Section 5. Finally, Section 6 offers concluding remarks.

2. Related Works, goals, and reference SIoE scenario

The integration of social networking and IoT solutions has been extensively examined in research, highlighting its potential to enhance networking services and foster new IoT applications. Early proposals primarily focused on incorporating social-like capabilities into IoT objects to improve trust among connected devices and enhance network navigability in large-scale environments [3]. Within this context, trustworthiness and resource availability are critical parameters that warrant thorough investigation. Researchers have introduced various strategies for evaluating trust management and the recommendations of entities within social networks and typical IoT environments. The paper [15] proposes a distributed trust model based on Markov chains to address security risks in the IoT. This model adapts an existing trust framework from Vehicular Ad hoc Networks (VANETs) for application within the IoT, utilizing an estimation algorithm to filter out malicious spam. The work presented in [16] introduces a Lightweight Hidden Markov Model for trust evaluation in IoT networks. This scheme employs a two-state Markov Model, consisting of Trusted and Compromised states, to assess the trustworthiness of network nodes. In [14], the authors propose a trust model for Social Internet of Things (SIoT) that merges social trust theory with the distinctive characteristics of IoT devices. This model captures competence, willingness, and social relationships to enhance service efficiency and security in the SIoT context. To manage a large number of nodes, strategies aimed at predicting trust and distrust values are essential. A focus on trust prediction is discussed in [17], where the authors propose a dynamic trust model that calculates both direct and indirect trust. This model combines exponential smoothing with a Markov chain to predict trustworthiness. Additionally, a time-aware smart object recommendation model is introduced in [18]. This study emphasizes the need for a recommendation system to assist users in discovering smart objects capable of providing services, addressing the challenges associated with collecting traditional user ratings or feedback. The paper [19] proposes a framework for creating, managing, controlling, and monitoring SIoT objects, facilitating the virtual representation of real-world objects as virtual entities for the composition of new services. This evaluation of virtual object selection during service provisioning aims to assess and understand latencies in the process. The contribution in [20] tackles challenges in SIoT, such as managing complex relationships and conserving energy resources. The proposed scenario considers object attributes, friend functions, and intelligent friend selection to optimize group messaging, enhancing communication reliability and improving service discovery efficiency in SIoT networks. More recently, the study presented in [21] introduces a recommendation model for SIoT services based on trust and Quality of Service (QoS). This approach integrates user trust connections and predicts QoS metrics, including service availability, reliability, and efficiency. In [22], the authors propose Trust–SIoT, an artificial neural network-based trust framework that integrates dynamic social trust metrics, including direct trust (current and historical interactions), reliability, benevolence, credible recommendations, and relationship degrees. Recommendations are obtained from trusted neighbors, and a SIoT knowledge graph is used to learn embedding vectors for quantifying relationships. The study in [23] introduces a deep learning-based semantic communication system with joint source-channel coding, channel adaptation, and bandwidth optimization, significantly improving transmission efficiency by enabling natural and rapid information exchange. Applied to the SIoT, this system ensures reliable, high-quality data transmission in diverse and complex environments, enhancing user experiences and supporting personalized services. However, scalability for large-scale SIoT deployments remains a critical challenge. The authors of [24] introduce the SIoT Community Detection Algorithm, aimed at enhancing service provision efficiency by streamlining service discovery and selection processes in SIoT environments optimizing service composition by minimizing execution time and reducing device distances required to fulfill user tasks.

Table 1 provides a summary of key works related to trust models in SIoT environments, highlighting their primary characteristics in terms of reliability (e.g., malicious behavior detection) and efficiency (e.g., QoS metrics analysis such as latency evaluation).

Ref.	Trust	Malicious Detection	QoS metrics	Predictive Model	Resources Evaluation
[15]	✓	✓			
[16]	✓	✓			
[14]	✓			✓	
[17]	✓			✓	
[18]	✓				
[19]	✓		✓		
[20]	✓		✓		
[21]	✓		✓	✓	
[22]	✓	✓		✓	
[23]	✓		✓	✓	
[24]	✓		✓		
This work	✓	✓	✓	✓	✓

Table 1: Trust models summary in Social Internet of Things environment.

2.1. Open issues covered by this contribution

In contrast to traditional strategies for securing networks, social-based predictions can offer more comprehensive insights into the experiences of entities [21]. Nevertheless, the aforementioned studies in this field present several unresolved issues and challenges for the scientific community. On one hand, they often require substantial computational resources, memory, or exhibit high complexity in evaluating entities, which can compromise network integrity, control, and performance. On the other hand, the inherent diversity of entities in such heterogeneous environments often leads researchers to focus narrowly on optimizing specific aspects of the service provisioning process, such as network latency or reliability. Thus, to the best of our knowledge, developing a statistical model that predicts the steady-state reputational behavior of a SIoE network—while simultaneously considering friendship relationships, trust parameters, and the available resources of service-providing nodes—remains a significant challenge.

With this in mind, this contribution aims to expand the scientific literature by proposing a Markov-based model that statistically analyzes the trustworthiness of service providers within a SIoE network. Specifically, the model presented in this paper explores the intricacies of the overall service provisioning process, capturing both the reputation and available resources of service providers registered in the social network of heterogeneous entities. This objective can be achieved while maintaining an acceptable level of complexity (as will be shown in Section 4.1), thereby enhancing practicality and efficiency, making the model applicable to real-world scenarios. Consequently, it can be effectively utilized to design and assess the capabilities of the SIoE network in delivering trusted services, while ensuring that the number of unserved service requests remains below specified thresholds.

2.2. Background on SIoE scenario

This work proposes a SIoE-based network architecture, illustrated in Figure 1, which consists of heterogeneous *social entities*. These entities can include individuals, physical devices (such as sensors, vehicles, and smartphones), software applications, processes, and data, interacting with one another to share information and content, collaborate on various tasks, and execute or provide services. The social entities are physically distributed across different geographical areas and, through their digital representation, can expose their attributes and features. By matching these attributes, they establish social relationships that reflect the level of trust shared among the participating entities. This process aids in identifying trusted candidates capable of fulfilling specific requests [26]. Within this composed Social Network, entities can function as both service requesters and service providers. Service providers share their resources and broadcast their availability to offer specific services, while service requesters communicate their needs. For this reason, each social entity specifies the list of services it can provide, enabling entities to join *service communities* based on shared application contexts and the services they can offer, thereby enhancing network navigability. Each service community is managed by a fog node that leverages the stored information related to entities' past experiences and the comprehensive set of attributes of registered social entities to operate the *Trust Management System (TMS)*. This system implements automated mechanisms to manage and calculate parameters associated with trust values. Selecting an appropriate trust metric is crucial for social entities, enabling them to make informed decisions regarding the most suitable service provider to meet their demands [27]. The overall system is overseen by upper-level fog nodes with greater storage capacities, which facilitate effective synchronization among the structures of distributed clusters through mutual interactions.

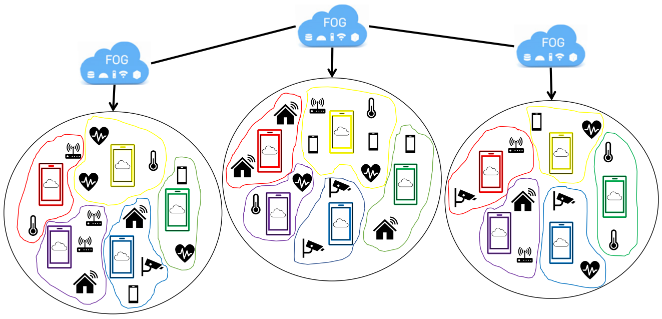


Figure 1: The SIoE reference environment.

2.3. Trust Management Procedure

The adopted Trust Management strategy extends beyond mere reliability and security by incorporating assessments of service trustworthiness and resource consumption. Figure 2 illustrates the service provisioning procedure, where a social entity sends a service request to the nearest fog node operating the TMS. The TMS generates a *trust ranking* for potential service providers and selects the most appropriate one for service execution. Additionally, it aids in identifying potential malicious social entities by excluding service providers that fall below a configured trust threshold during the selection process. According to our recent, albeit preliminary, conference papers [28, 29], the trustworthiness level of a service provider is dependent on feedback from past interactions between entities, which collects information about the services provided. The resulting Trust value $Tr_{ij}(t)$ is determined by two primary factors when considering the i-th social entity requesting a service and the j-th social entity as a potential provider. The first factor is the Sociality factor S_{ij}, which reflects the level of friendship between the entities and categorizes established relationships by their importance [30]. The second factor is the Reputation Factor $R_j(t)$, which is derived from feedback received from prior interactions up to the time instant t. This factor evolves dynamically over time and is modeled as a linear combination of three primary components:

- direct feedback: represents how the requester evaluated the provider based on their service provision.
- indirect feedback: reflects the evaluations provided by the requester's friends regarding the provider.
- indirect non-friend feedback: captures the evaluations from other non-friend social entities regarding the provider.

Further details on this formulation and its application can be found in our previous work [28]. The Trust value is ultimately calculated as follows: $Tr_{ij}(t) = S_{ij} \cdot R_j(t)$.

Additionally, the designed TMS enhances the process by assessing the resource capability of social objects to prevent service execution failures or unavailability due to insufficient resources, which is critical in environments where network participants may have limited capabilities. After computing the trust ranking, the resource capacity of the candidate provider is verified to ensure that sufficient resources are available for service execution. If this check fails, the candidate provider is temporarily removed from the list. Subsequently, the service requester submits feedback to the system, providing an evaluation of the service provider. This feedback is represented as a quantitative value that reflects the requester's level of satisfaction with both the quality and reliability of the service delivered. Then it is stored for future evaluations in the fog node. Many valuable state-of-the-art studies, such as the one proposed in [31], focus on analyzing feedback evaluation in detail. Without loss of generality, this work defines a threshold to classify feedback as either positive or negative. Specifically, feedback values exceeding this threshold are considered positive, while those falling below are categorized as negative. Finally, the TMS interfaces with the upper-level fog node, which maintains a distributed database containing information about the relationships and reputations of social entities. This interface facilitates synchronization between different geographical clusters. This scalable double-clustered framework leverages fog computing to enable the responsive dissemination of real-time trustworthiness information for entities within a SIoE environment [32].

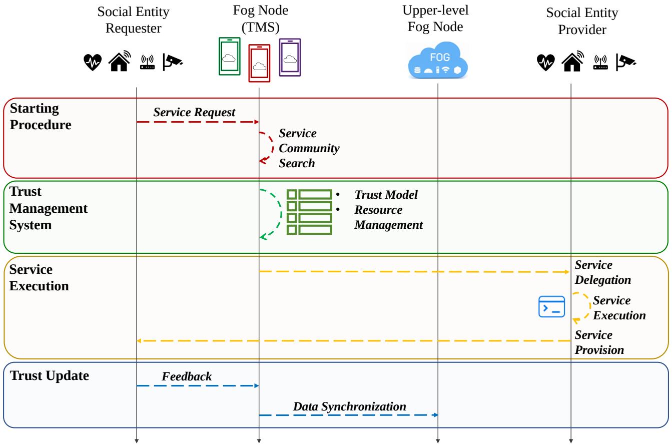


Figure 2: The designed Trust Management System procedure.

3. Modelling a social entity through Markov Theory

To achieve the objectives of this contribution and predict the behavior of an entity within a SIoE environment, a novel Markov chain model is formulated. As is well known, Markov chains are particularly useful for investigating systems that exhibit a degree of randomness or uncertainty [33]. In this context, the proposed Markov chain evaluates trust and resource properties associated with a social entity. This evaluation can be readily extended to the entire Social Network by considering an independent Markov chain for each involved entity.

With reference to the j-th candidate provider entity in the Social Network, each state of the Markov chain consists of a triad of values, represented as (p_j, T_j, c_j). Specifically, p_j denotes the number of positive feedbacks received based on past actions, T_j specifies the total number of services offered, and c_j indicates the resources currently allocated to provide these services. It is important to note that, by design, since the feedback received can be mapped in a binary value (positive or negative), it depends on the probability of each entity in the network providing the service correctly. In the considered model, this probability, denoted as P_{pf}, is influenced not only by the ethical behavior of the entity within the network but also by its capabilities, which may vary. Therefore, since the evaluation provided by the requester is considered honest, the probability of receiving negative feedback is influenced not only by malicious intent but also by potential errors on the part of the provider. These errors, however, are not necessarily indicative of an attack on the system's trustworthiness but may result from factors such as service delivery failures or resource limitations. The last parameter of the triad, in fact, highlights the heterogeneous nature of the entities, as they exhibit varying capacities and can offer different amounts of resources. For the sake of generality, and based on the classification outlined in [34], smart IoE entities can be categorized into several distinct groups. These include Low-end IoE devices, characterized by limited resources (e.g., the Open Mote); Middle-end IoE devices, which provide more features and better processing capabilities compared to Low-end devices (e.g., the Arduino); and High-end IoE devices, dis-

Table 2: Main Symbols Description.

Symbol	**Meaning**
Tr_{ij}	Trust level of i towards the entity j
S_{ij}	Sociality factor measuring the friendship ties between i and j
R_j	Reputation factor of the entity j
$\gamma_{A\to B}$	Transition rate from the state A to the state B
Λ	Total number of service requests
λ	Average number of service requests per unit of time
μ	Average number of requesters served per unit of time
λ_j	Average number of service requests assigned to the entity j
$1/\mu_j$	Average service rate employed by the entity j to perform a service
$P(Req_{i\to j})$	Probability that a service request from i is assigned to provider j
N	Number of social entities belonging a service community
C_j	Maximum number of allocable resources of the j-th social entity
ϕ	set of entities owning a Trust value with i greater than Tr_{ij}
$P_{a=n}(\delta)$	Probability of n arrival in δ
$P_{s=n}(\delta)$	Probability of n task accomplished in δ
P_{nf}	Probability to receive a negative feedback
P_{pf}	Probability to receive a positive feedback
$\mathcal{F}_i$	Set of friends of the i-th requester
$\mathcal{F}_j$	Set of friends of the j-th provider
$P_B(j)$	Blocking probability of the j-th provider
R_{loss}	Reputation Loss Percentage
$E[R_j\|T_j]$	Average Reputation of the j-th provider
$L(T_j)$	Intensity of unserved requests
T_Δ	Number of received feedback at steady state
$A_{j_{he}}(T_{j_{he}})$	Probability that an high-end provider is available to perform a request

tinguished by substantial resources and storage capacity (e.g., smartphones). To address these differences, the proposed model assigns distinct values for maximum allocable resources (denoted as C_j) to each social entity based on its capabilities, as determined by its class.

Figure 4 illustrates the complete sequence of states in the Markov chain. In this graph, the edges are labeled with the transition rates between states. Without loss of generality, we assume that service requests are generated according to a Poisson distribution with a rate parameter λ. Furthermore, the inter-arrival times and service times are considered to be statistically independent. Table 2 summarizes the key symbols used to describe the model along with their meanings.

Given the current state (p_j, T_j, c_j), the proposed model can yield important insights into the behavior of a social entity from both trustworthiness and resource perspectives. Specifically, it can determine whether a node is acting appropriately or maliciously by evaluating its average reputation. Furthermore, the model can assess the entity's availability by analyzing the number of requests it has successfully fulfilled versus those that remain unserved. The remainder of this section outlines the methodology used to obtain the state probabilities of the entities, as schematically shown in Figure 3. Specifically, starting from the known current state, the proposed model calculates the rate of requests that could be assigned to the j-th evaluated provider, denoted as λ_j. Subsequently, using λ_j along with the service time required to fulfill a request, the evaluation of transition rates enables the prediction of state probabilities. This, in turn, facilitates the extraction of insights regarding the potential behaviors that an entity may exhibit.

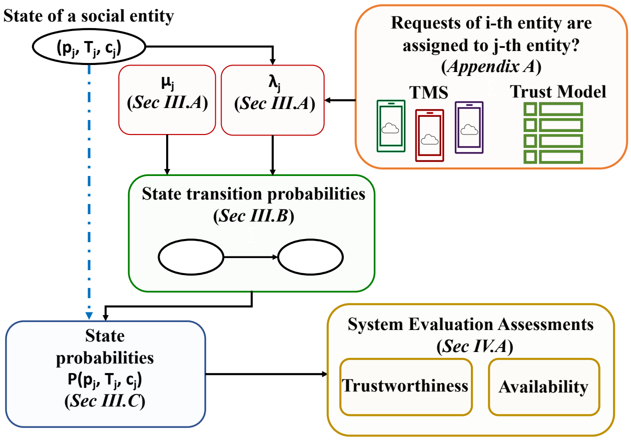

State of a social entity
(p_j, T_j, c_j)
μ_j (Sec III.A)
λ_j (Sec III.A)
Requests of i-th entity are assigned to j-th entity? (Appendix A)
TMS
Trust Model
State transition probabilities (Sec III.B)
State probabilities P(p_j, T_j, c_j) (Sec III.C)
System Evaluation Assessments (Sec IV.A)
Trustworthiness
Availability

Figure 3: The complete conceived methodology.

3.1. Evaluation of the average number of service requests assigned to a social entity

Let N be the number of social entities belonging to a service community. For each entity $j \in N$, let (p_j, T_j, c_j) represent the triad that characterizes its current state. Additionally, let $\mathcal{F}_j$ denote the set of entities that have a social relationship with entity j, defined as:

$$\mathcal{F}_j = \{\forall n \in N \mid S_{nj} \geq 0\}. \tag{1}$$

Assuming that the social entity requesting the service is $i \in \mathcal{F}_j$, the average number of service requests assigned to the j-th social entity, denoted as λ_j, can be computed using the following formula:

$$\lambda_j = \sum_{i=1}^{|\mathcal{F}_j|} \lambda_{ij} \cdot P(Req_{i\to j}|(p_j, T_j, c_j)), \tag{2}$$

where λ_{ij} is the average number of service requests originating from the i-th social entity that can be assigned to the j-th provider, and $P(Req_{i\to j})$ is the probability that the TMS selects the j-th social entity as the most suitable provider.

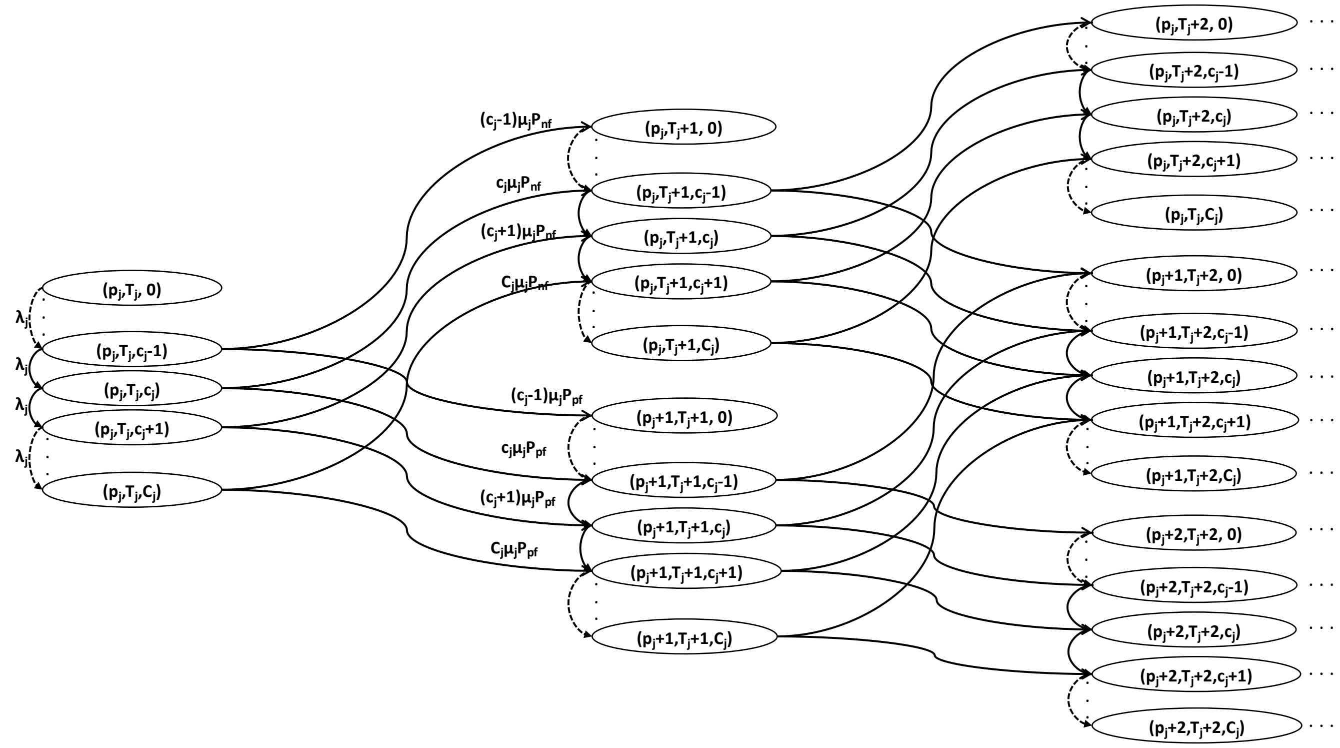


Figure 4: State Diagram of the proposed model.

Now, let $\mathcal{F}_i$ be the set of entities that have a social relationship with the i-th requester, defined as:

$$\mathcal{F}_i = \{\forall n \in N \mid S_{ni} \geq 0\}. \tag{3}$$

Let ϕ_i be the set of social entities that are perceived as more trusted than the j-th entity according to the i-th requester's opinion, defined as:

$$\phi_i = \{\forall n \in \mathcal{F}_i \mid Tr_{in} \geq Tr_{ij}\}. \tag{4}$$

To calculate the probability that a request coming from i is assigned to j, denoted by $P(Req_{i\to j})$, the Total Probability Law is applied across all possible cardinalities of the set ϕ_i. The resulting probability can be expressed as:

$$\lambda_j = \sum_{i=1}^{|\mathcal{F}_j|} \lambda_{ij} \sum_{n=0}^{|\mathcal{F}_i|} P(Req_{i\to j} \big| (p_j, T_j, c_j), |\phi_i| = n). \tag{5}$$

In the interest of clarity, the mathematical steps for developing Equation 5 will be relegated to *Appendix A*.

It is evident that the probability expressed by $P(Req_{i\to j})$ is linked to the comparison of trustworthiness values of all available service providers at the moment the service request arrives. Based on the trust model introduced in the TMS discussed in Section 2.3, and leveraging the parameters of the triad that represents the state of an entity, the trust value of a service provider can be defined as follows:

Definition 1. Given the triad (p_j, T_j, c_j) representing the state of the j-th service provider, and the Sociality factor S_{ij}, which quantifies the strength of the friendship ties between the i-th and j-th social entities, the Trust value Tr_{ij} can be expressed as: $Tr_{ij} = S_{ij} \cdot R_j$, where $R_j = \frac{p_j}{T_j}$ represents the Reputation Factor of the j-th entity. This Reputation Factor R_j reflects the proportion of positive feedback (p_j) out of the total number of services provided (T_j), thus capturing the historical performance of the service provider based on past interactions and evaluations.

In this context, μ_j is introduced as the average service rate representing the number of service requests the j-th entity can handle per unit of time. Mathematically, μ_j is the reciprocal of the service time required by the j-th provider to fulfill a request. Here, while C_j represents the maximum allocable resources for a service provider, μ_j quantifies the efficiency with which the provider can serve requests. Both parameters, C_j and μ_j, are defined according to the classification of social entities outlined in [34], which categorizes entities into different classes based on their resource capabilities. In the model development, the values of (C_j, μ_j) are assumed to be fixed for each class of entity, reflecting the inherent capabilities of each service provider. Specific numerical values for these parameters will be provided in the Section 5, illustrating how they influence the overall service performance of the network.

3.2. States Transition Rates

As discussed in Section 3.1, the parameters λ_j and μ_j play a crucial role in governing the dynamics of these transitions. The variation in the triad (p_j, T_j, c_j), which represents the current state of the social entity, directly impacts the selection process for the most suitable service provider for future requests.

The state transition diagram of a generic node is depicted in Figure 5. The conceived model accounts for the following three types of events: (i) the TMS assigns a service request to the j-th entity provider, (ii) the reception of positive feedback in response to a service provided, and (iii) the reception of negative feedback following a service provided.

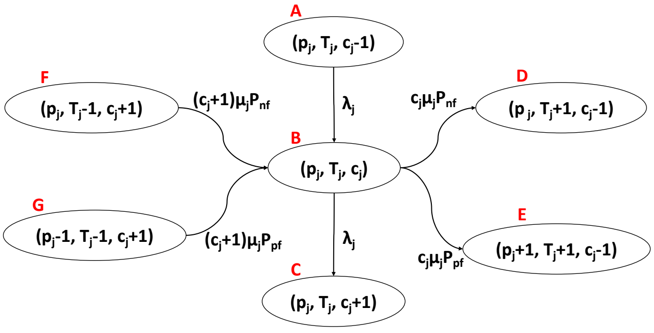

A
$(p_j, T_j, c_j\text{-}1)$
F
$(p_j, T_j\text{-}1, c_j\text{+}1)$
$(c_j\text{+}1)\mu_jP_{nf}$
λ_j
$c_j\mu_jP_{nf}$
D
$(p_j, T_j\text{+}1, c_j\text{-}1)$
B
(p_j, T_j, c_j)
G
$(p_j\text{-}1, T_j\text{-}1, c_j\text{+}1)$
E
$(c_j\text{+}1)\mu_jP_{pf}$
λ_j
$c_j\mu_jP_{pf}$
$(p_j\text{+}1, T_j\text{+}1, c_j\text{-}1)$
C
$(p_j, T_j, c_j\text{+}1)$

Figure 5: Transition rate diagram of j-th provider.

3.2.1. Case 1: the TMS assigns a service request to the j-th entity provider.

In reference to the states illustrated in Figure 4, all downward edges correspond to the assignment of a service task to the j-th provider.

Theorem 1. *Let $(p_j, T_j, c_j - 1)$ represent the generic state A of the j-th social entity. Given C_j as the maximum number of allocable resources for the considered entity and $P_{A\rightarrow B}$ as the probability of transitioning from state A to B (characterized by the triad (p_j, T_j, c_j)), the transition rate $\gamma_{A\rightarrow B}$ from state A to state B can be expressed as:*

$$\gamma_{A\rightarrow B} = \gamma_{(p_j,T_j,c_j-1)\rightarrow(p_j,T_j,c_j)} = \begin{cases} 0 & if \quad c_j = C_j, \\ \lambda_j & if \quad c_j < C_j. \end{cases} \tag{6}$$

Proof. Considering the transition resulting from the assignment of a service, it will consequently lead to the utilization of a free resource of the j-th entity. Accordingly, the resulting state will be represented by the triad (p_j, T_j, c_j). However, if the parameter pertaining to the currently allocated resources has reached its maximum value C_j, the task cannot be assigned to the j-th entity, and the transition cannot occur. Thus, the transition rate $\gamma_{A\rightarrow B}$, which quantifies the probability per unit of time of an event occurring (e.g., the state transition due to service assignment) within an infinitesimally time interval δ, is defined as: $\gamma_{(p_j,T_j,c_j-1)\rightarrow(p_j,T_j,c_j)} = \lim_{\delta\rightarrow 0} \frac{P_{A\rightarrow B}(\delta)}{\delta}$ if $c_j < C_j$ and equal to 0 if $c_j = C_j$. This limit represents the probability that one service is assigned to the j-th entity (denoted as $P_{a=1}(\delta)$), while no services are accomplished (denoted as $P_{s=0}(\delta)$) during a time interval of length δ. Assuming that these probabilities are independent, the previous equation can be rewritten as: $\lim_{\delta\rightarrow 0} \frac{P_{a=1}(\delta)\cdot P_{s=0}(\delta)}{\delta}$. Given that the inter-arrival and service times are assumed to follow an exponential distribution, with arrival and conditional service rates governed by a Poisson process, the corresponding probabilities can be expressed as follows: $P_{a=1}(\delta) = \lambda_j\delta \cdot e^{-\lambda_j\delta}$ and $P_{s=0}(\delta) = (e^{-\mu_j\delta})^{c_j-1}$. Consequently, the aforementioned limit can be calculated as:

$$\lim_{\delta\rightarrow 0} \frac{\lambda_j\delta \cdot e^{-\lambda_j\delta} \cdot (e^{-\mu_j\delta})^{c_j-1}}{\delta} = \lambda_j.$$

□

3.2.2. Case 2: negative feedback reception in response to a service provided.

With reference to Figure 4, all the edges progressing upward forward indicate the reception of negative feedback in response to successful service delivery.

Theorem 2. *Let (p_j, T_j, c_j) represent the generic state B of the j-th social entity, and let P_{nf_j} denote the probability of receiving negative feedback due to successful service execution. Given C_j as the maximum number of allocable resources for the considered entity and $P_{B\rightarrow D}$ as the probability of transitioning from state B to D (characterized by the triad $(p_j, T_j + 1, c_j - 1)$), the corresponding transition rate $\gamma_{B\rightarrow D}$ can be expressed as follows:*

$$\gamma_{B\rightarrow D} = \gamma_{(p_j,T_j,c_j)\rightarrow(p_j,T_j+1,c_j-1)} = \\ = \begin{cases} 0 & if \quad c_j = 0, \\ c_j \cdot \mu_j \cdot P_{nf_j} & if \quad 0 < c_j < C_j. \end{cases} \tag{7}$$

Proof. Considering the j-th entity in the state described by the triad (p_j, T_j, c_j), when a task is completed, feedback is received. If the feedback is negative, the number of positive evaluations remains unchanged, while the total number of evaluations increases. Additionally, upon successful completion of the service, the j-th social entity releases an allocated resource, which becomes available again. Therefore, the new state after this transition will be $(p_j, T_j + 1, c_j - 1)$. However, if $c_j = 0$, this indicates that the entity j is not currently engaged in any service and, consequently, will not receive any feedback. The transition rate $\gamma_{B \to D}$, which measures the probability per unit of time that an event occurs (such as a state transition due to the reception of negative feedback) within an infinitesimally small time interval δ, is defined as: $\gamma_{(p_j,T_j,c_j)\to(p_j,T_j+1,c_j-1)} = \lim_{\delta\to 0} \frac{P_{B\to D}(\delta)}{\delta}$, if $0 < c_j < C_j$, and equal to 0 if $c_j = 0$. This limit represents the probability that no new services are assigned to the considered entity (denoted as $P_{a=0}(\delta)$), and that one service is successfully completed, accompanied by the reception of negative feedback (denoted as $P_{s=1}(\delta)$), within a time interval δ. Assuming these two probabilities are independent, and defining P_{nf_j} as the probability of receiving negative feedback for the j-th entity, the previous equation can be rewritten as:

$$\gamma_{(p_j,T_j,c_j)\to(p_j,T_j+1,c_j-1)} = \lim_{\delta\to 0} \frac{P_{a=0}(\delta) \cdot P_{s=1}(\delta) \cdot P_{nf_j}}{\delta}. \tag{8}$$

Given that the inter-arrival and service times are assumed to be exponential, and the arrival and service rates follow Poisson distributions, the probabilities can be expressed as: $P_{a=0}(\delta) = e^{-\lambda_j \delta}$ and $P_{s=1}(\delta) = c_j \cdot (1 - e^{-\mu_j \delta}) \cdot e^{-\mu_j \delta (c_j - 1)}$. Substituting these into the Equation 8, the following formula is obtained:

$$\lim_{\delta\to 0} \frac{e^{-\lambda_j \delta} \cdot c_j \cdot (1 - e^{-\mu_j \delta}) \cdot e^{-\mu_j \delta (c_j-1)} \cdot P_{nf_j}}{\delta} \tag{9}$$

Since $e^{-\lambda_j \delta} \to 1$ as $\delta \to 0$, and $1 - e^{-\mu_j \delta} \approx \mu_j \delta$, the expression simplifies to: $\lim_{\delta\to 0} \frac{c_j \cdot \mu_j \delta \cdot P_{nf_j}}{\delta} = c_j \cdot \mu_j \cdot P_{nf_j}$ Thus, the transition rate $\gamma_{(p_j,T_j,c_j)\to(p_j,T_j+1,c_j-1)}$ is:

$$\gamma_{(p_j,T_j,c_j)\to(p_j,T_j+1,c_j-1)} = c_j \cdot \mu_j \cdot P_{nf_j}.$$

□

3.2.3. Case 3: positive feedback reception in response to a service provided.

Differently from the *Case 2*, as illustrated in Figure 4, all the edges progressing downward correspond to the successful completion of a service accompanied by the reception of positive feedback.

Theorem 3. *Let (p_j, T_j, c_j) be the generic state B of the j-th social entity. Given C_j as the maximum number of allocable resources for the considered entity and $P_{B\to E}$ as the probability of transitioning from state B to E, represented by the triad $(p_j + 1, T_j + 1, c_j - 1)$, the transition rate $\gamma_{B\to E}$ can be expressed as:*

$$\begin{aligned} \gamma_{B\to E} &= \gamma_{(p_j,T_j,c_j)\to(p_j+1,T_j+1,c_j-1)} = \\ &= \begin{cases} 0 & if \quad c_j = 0, \\ c_j \cdot \mu_j \cdot P_{pf_j} & if \quad 0 < c_j < C_j. \end{cases} \end{aligned} \tag{10}$$

Proof. When a service is successfully accomplished and positive feedback is received, both the number of positive evaluations p_j and the total evaluations T_j for the j-th social entity increase by 1. Additionally, upon service completion, the j-th social entity releases one of its employed resources, reducing c_j by 1. Therefore, the new state after this transition is represented by the triad $(p_j + 1, T_j + 1, c_j - 1)$. However, if the parameter representing the currently allocated resources, n_j, is equal to 0, this indicates that the j-th entity is not currently performing any tasks. Consequently, no state transition can occur under these circumstances. The transition rate $\gamma_{B\to E}$, which measures the probability per unit time that a state transition occurs due to the reception of positive feedback within an infinitesimally small time interval δ, can be mathematically expressed as follows:$\gamma_{(p_j,T_j,c_j)\to(p_j+1,T_j+1,c_j-1)} = \lim_{\delta\to 0} \frac{P_{B\to E}(\delta)}{\delta}$, if $0 < c_j < C_j$. If $c_j = 0$, meaning no resources are currently allocated, the transition rate is equal to 0, as no feedback can be received when the entity is not performing any tasks. This limit can be derived using a similar approach to that followed in the previous theorem, with the sole difference being the consideration of the probability of receiving positive feedback. Consequently, it can be explicitly expressed as: $\lim_{\delta\to 0} \frac{e^{-\lambda_j \delta} \cdot c_j \cdot (1 - e^{-\mu_j \delta}) \cdot (e^{-\mu_j \delta (c_j - 1)}) \cdot P_{pf_j}}{\delta} = c_j \cdot \mu_j \cdot P_{pf_j}$.

□

Corollary 3.1. Each state transition related to service accomplishment and feedback reception follows a similar calculation methodology. These transitions are influenced by the resources currently allocated, as indicated in the triad representing the state of the j-th entity, and depend on both the entity's service rate μ_j, and the probability of receiving either a positive or negative feedback. All the transition rates are depicted in the state diagram shown in Figure 5.

3.3. State Probability

Building upon the estimation of transition rate probabilities evaluated in the previous section, the focus now shifts to calculating the state probabilities of the designed Markov chain. In this context, each state represents the condition of an entity, encompassing evaluations received from past experiences and resources allocated for executing services.

Theorem 4. *Given the state (p_j, T_j, c_j) of the j-th social entity, let λ_j and μ_j be the average number of service requests assigned to the j-th entity and the average service rate employed by the j-th entity, respectively. Assuming the transition rates are calculated as described in Section 3.2, the state probability describing the behavior of the j-th social entity can be summarized by the following equation:*

$$\begin{aligned} P(p_j, T_j, c_j) &= P(p_j, T_j, c_j - 1) \cdot \frac{\lambda_j}{\lambda_j + (c_j - 1) \cdot \mu_j} + \\ &+ P(p_j, T_j - 1, c_j + 1) \cdot \frac{(c_j + 1) \cdot \mu_j \cdot P_{nf_j}}{\lambda_j + (c_j + 1) \cdot \mu_j} + \\ &+ P(p_j - 1, T_j - 1, c_j + 1) \cdot \frac{(c_j + 1) \cdot \mu_j \cdot P_{pf_j}}{\lambda_j + (c_j + 1) \cdot \mu_j}. \end{aligned} \tag{11}$$

where $0 \le p_j \le T_j$ and $0 \le c_j \le C_j$. If the state probability arguments do not satisfy these inequalities, the corresponding probability is equal to 0.

Proof. This theorem articulates the behavior of a social entity using a recursive formula applicable to any state within the Markov chain. Starting from an initial state with a probability of one, each state can be expressed as a function of its predecessor, adhering to the principles of the Markov process. Specifically, the probability of the generic state (p_j, T_j, c_j) (as illustrated in Figure 5) is computed by applying the Total Probability Law across all possible current states: $P(p_j, T_j, c_j) = \sum_{s=1}^{S} P((p_j, T_j, c_j)|\sigma_s)$, where σ_s denotes the s-th state that transitions into the (p_j, T_j, c_j) state. By leveraging the definition of conditional probability, the equation can be reformulated as: $P(p_j, T_j, c_j) = \sum_{s=1}^{S} P((p_j, T_j, c_j)|\sigma_s) \cdot P(\sigma_s)$.

In this context, the conditional probability $P((p_j, T_j, c_j)|\sigma_s)$ can be determined using the empirical definition of probability. This approach assesses the likelihood of an event occurring based on the ratio of favorable outcomes to the total number of possible outcomes. Specifically, the probability of transitioning to the state (p_j, T_j, c_j) from the originating state σ_s can be can be expressed as the transition rate $\gamma_{\sigma_n \to (p_j, T_j, c_j)}$, divided by all the possible transition rates departing from the state σ_s. Therefore, let $P(p_j, T_j, c_j - 1)$, $P(p_j, T_j - 1, c_j + 1)$, and $P(p_j - 1, T_j - 1, c_j + 1)$ represent the probabilities of the states transitioning into (p_j, T_j, c_j), the (p_j, T_j, c_j) can be written as reported in the Equation.11. In this expression, the denominator $\lambda_j + (c_j + 1)\mu_j$ accounts for the total transition rates associated with the state (p_j, T_j, c_j). Specifically, $\lambda_j + (c_j + 1) \cdot \mu_j \cdot P_{nf_j} + (c_j + 1) \cdot \mu_j \cdot P_{pf_j} = \lambda_j + (c_j + 1) \cdot \mu_j \cdot (P_{nf_j} + P_{pf_j})$. Since $(P_{nf_j} + P_{pf_j}) = 1$, the equation simplifies to: $\lambda_j + (c_j + 1) \cdot \mu_j$.

□

4. Model Applicability and Complexity Analysis

This section aims to elucidate the insights gained from the model's outcomes. Specifically, it is helpful in evaluating the following aspects: the average reputation of a social entity, the intensity of unserved requests, the establishment of a reputation threshold, and the probability of availability of higher-class services.

1. **Average reputation.** As described in Definition 1, the Reputation Factor plays a critical role in establishing the trustworthiness of stakeholders, influencing the selection of the most appropriate service provider. Given p_j as the number of positive feedbacks and T_j as the total number of feedbacks received by a social entity, the expected value of the reputation R_j can be computed as follows: $E[R_j|T_j] = \sum_{p_j=0}^{T_j} \frac{p_j}{T_j} P(p_j|T_j)$. In this context, for a fixed T_j, the probability $P(p_j|T_j)$ in the aforementioned equation serves as the weight for the reputation values that a social entity may attain. By explicitly defining this probability, the average reputation of an entity can be computed as follows:

$$E[R_j|T_j] = \sum_{p_j=0}^{T_j} \frac{p_j}{T_j} \frac{\sum\limits_{c_j=0}^{C_j} P(p_j, T_j, c_j)}{\sum\limits_{p_j=0}^{T_j} \sum\limits_{c_j=0}^{C_j} P(p_j, T_j, c_j)}. \tag{12}$$

2. **Intensity of unserved requests on the SIoE Network.** As detailed in Section 3, c_j denotes the quantity of resources currently utilized by the j-th entity. In this context, the probability of being in a state characterized by the maximum value of c_j (i.e., $c_j = C_j$) corresponds to the likelihood that a new incoming request directed to the j-th entity is rejected due to insufficient resources. This analysis provides an opportunity to explore the intensity of unserved requests within the social network. Let N represent the total number of social entities within a service community. Given $P(p_j, T_j, C_j)$ as the state probability, and assuming a fixed T_j, the intensity of service requests that cannot be fulfilled, denoted by $L(T_j)$, can be expressed as follows:

$$L(T_j) = \sum_{j=1}^{N} \lambda_j (p_j, T_j, C_j) \frac{\sum\limits_{p_j=0}^{T_j} P(p_j, T_j, C_j)}{\sum\limits_{p_j=0}^{T_j} \sum\limits_{c_j=0}^{C_j} P(p_j, T_j, c_j)}. \tag{13}$$

3. **Reputation threshold.** The proposed model can also be utilized to establish a reputation threshold, thereby highlighting its significance within the social network. To this end, it is essential to define the number of feedbacks received, denoted as T_Δ, beyond which the analysis can be deemed adequate for providing a robust evaluation of the conduct of the social entity. Considering p_0 and T_0 as the initial values related to positive feedback and the total feedback received, the percentage of reputation loss for a social entity, denoted as R_{loss}, can be expressed through the inequality: $\frac{\overline{p_j}}{T_j} \leq R_{loss} \cdot \frac{p_0}{T_0}$, where $\overline{p_j}$ represents the average number of received positive feedbacks. In particular, it becomes counterproductive to consider social entities with a reputation below the threshold defined by R_{loss} in the service provisioning process. Such entities can consequently be categorized as malicious. Assuming $T_j = T_0 + T_\Delta$ and let $\overline{p_j}$ expressed as: $\overline{p_j} = p_0 + T_\Delta \cdot P_{pf_j}$. Isolating T_Δ in the previous inequality, we can reformulate it as follows:

$$T_\Delta \geq \frac{p_0 - R_{loss} \cdot p_0}{(\frac{R_{loss} p_0}{T_0}) - P_{pf_j}}, \tag{14}$$

4. **Probability that an higher-class provider is available to perform a request.** By examining the states of the Markov chain, the proposed model serves as an effective tool for monitoring the likelihood that a service provider within a service community possesses the requisite re-

sources to fulfill a service request. Specifically, in accordance with the categorization outlined by [34], the proposed Markov chain can be evaluated in a way that highlights the highest-performing entities. Assigning requests to devices with elevated computing capabilities can enhance network efficiency, facilitating quicker processing of service requests and decreasing the incidence of unserved requests. In this context, and considering a fixed T_j, the availability of the j_{he}-th high-end service provider, denoted by $A_{j_{he}}(T_{j_{he}})$, can be articulated in terms of the probability: $\sum_{p_{j_{he}}=0}^{T_{j_{he}}} \sum_{c_{j_{he}}=0}^{C_{j_{he}}-1} P(p_{j_{he}}, T_{j_{he}}, c_{j_{he}} | T_{j_{he}})$. Transitioning from conditional probability to joint probability and explicitly incorporating $P(T_{j_{he}})$, the final expression can be articulated as follows:

$$A_{j_{he}}(T_{j_{he}}) = \frac{\sum_{p_{j_{he}}=0}^{T_{j_{he}}} \sum_{c_{j_{he}}=0}^{C_{j_{he}}-1} P(p_{j_{he}}, T_{j_{he}}, c_{j_{he}})}{\sum_{p_{j_{he}}=0}^{T_{j_{he}}} \sum_{c_{j_{he}}=0}^{C_{j_{he}}} P(p_{j_{he}}, T_{j_{he}}, c_{j_{he}})}. \quad (15)$$

4.1. Complexity evaluation

As detailed in the preceding sections, the proposed methodology calculates state probabilities based on the triad of a state (p_j, T_j, c_j), facilitating the analysis of trust and availability in social entities. In this context, it is crucial to consider the computational complexity of Equation 11 to make informed decisions regarding its practical application and ensure efficient integration into the intended environment.

Considering the Markov property, which asserts that the future state of the process depends solely on its present state, assessing the complexity of the entire model entails calculating the complexity of all incoming state probabilities along with the corresponding state transition rates for every state within the chain. Specifically, let t represent the number of steps required to construct the Markov chain. To reach the steady-state at step T_Δ, $(t+1)$ backward recursions are required, and at each step, we account for $C_j + 1$ resources in order to determine the complete set of state probabilities.

Additionally, the computational complexity associated with the evaluation of the state transition rates necessitates counting the number of elementary operations involved, denoted as N_{λ_j}, for the computation of λ_j. Consequently, the total number of elementary operations required to determine the steady-state probabilities, referred to as N_{ss}, can be bounded as follows:

$$N_{ss} < \sum_{t=0}^{T_\Delta} (t+1)(C_j + 1) N_{\lambda_j} \quad (16)$$

Explicitly, the number of elementary operations N_{λ_j} is of the order $O(|\mathcal{F}_i|^3 \cdot |\mathcal{F}_j| \cdot \nu_0)$, where $|\mathcal{F}_i|$ and $|\mathcal{F}_j|$ represent the cardinalities of the respective sets. A detailed explanation of this result can be found in Appendix B. By substituting these expressions into Equation 16, the resulting formula is obtained as follows:

$$\begin{aligned} N_{ss} &< \sum_{t=0}^{T_\Delta} (t+1)(C_j+1)(|\mathcal{F}_i|^3 |\mathcal{F}_j| \nu_0) = \\ &= (C_j+1)(|\mathcal{F}_i|^3 |\mathcal{F}_j| \nu_0)\Big(1 + \sum_{t=1}^{T_\Delta} t + 1\Big) = \\ &= (C_j+1)(|\mathcal{F}_i|^3 |\mathcal{F}_j| \nu_0)(1 + \frac{T_\Delta}{2}(T_\Delta + 1) + T_\Delta) = \\ &= (C_j+1)(|\mathcal{F}_i|^3 |\mathcal{F}_j| \nu_0)(1 + \frac{T_\Delta^2}{2} + \frac{3T_\Delta}{2}) \end{aligned} \quad (17)$$

Since C_j is, by design, significantly smaller than the other quantities, Equation 17 indicates that the overall computational complexity of the procedure is of the order:

$$O(|\mathcal{F}_i|^3 \cdot |\mathcal{F}_j| \cdot \nu_0 \cdot T_\Delta^2).$$

Moreover, it is important to note that, since the Markov chain for the single social entity is evaluated in a limited geographical cluster of the framework detailed in Section 2.3, the range of possible values for $|\mathcal{F}|$, ν, and T_Δ is inherently constrained to hundreds and tens by design, making the computations manageable for modern computing systems. This characteristic allows for the implementation of the proposed methodology without reliance on more complex tools or dynamic programming approaches, which could increase the complexity and hinder practical applicability. Furthermore, avoiding such methods helps to circumvent potential convergence time issues that may arise from more elaborate computational strategies.

5. Model validation and analysis

This section evaluates the proposed model and analyzes the results obtained. First, the analytical Markov chain-based model is validated by comparing its results against heuristic approaches and simulation solutions to ensure that the model accurately reflects the environmental behavior. Second, various network configurations based on real-world scenarios are examined to assess the overall network performance.

Table 3: Social Entities resources and capabilities

(a) Services Parameter

Type of Service	Resource Consumption	Information Size[Mbit]
High-end service	0.3	1.4
Middle-end service	0.2	1
Low-end service	0.1	0.6

(b) Device Parameter

Social Entity Class	Res. Capab.	Clock [Mcyc./s]	C_j	μ
High-end dev.	0.9	2000	3	1.428
Middle-end dev.	0.6	1000	2	0.714
Low-end dev.	0.2	40	1	0.025

5.1. *Parameter setup*

The validation of the proposed Markov chain-based model is a critical step in this research process, as it enables the assessment of the model's accuracy and its capacity to effectively capture the behavior of social entities.

To achieve this, this study employs a simulator developed in C++ to compare the findings of [28] and [29] with the proposed analytical model. Specifically, the SIoE simulator is designed to replicate the service provisioning process within a Social Network of social entities organized into logical clusters, each comprising service communities defined by the types of services they can handle. For this analysis, given that the focus is on a single type of service, only one service community is simulated. In this context, the SIoE simulator accommodates three distinct types of services: High-end, Middle-end, and Low-end services. Table 3 provides detailed information regarding each type of service and corresponding social entity class. Specifically, Table 3a presents the resource consumption associated with each type of service, which ranges from 0.1 to 0.3, alongside the bit size of the information to be processed, as outlined in the classification by [34]. In contrast, Table 3b details the resource capabilities of each class of social entity, which range from 0.2 to 0.9, along with their clock speeds, measured in Megacycles per second. Additionally, it defines values for the pair (C_j, μ_j), which represent the maximum allocable resources and the average service rate utilized in the Markov chain, respectively.

Service requests are generated according to a Poisson distribution, with an average rate λ ranging from 3 to 22 requests per second. This variation in request rates enables the assessment of network performance under different traffic loads. To ensure robust results, data from each simulated scenario are collected using 10 different random seeds, allowing for diverse distributions of social relationships and service requests. Furthermore, the analysis involves 25 social entities evenly distributed across the High-end and Middle-end classes within a High-end service community cluster. A fixed percentage of these entities is designated as malicious, intentionally providing poor services. In conjunction with the computer simulation, the behavior of each social entity is analyzed through its corresponding Markov chain, constructed using the analytical model presented. For the construction of these chains, the initial parameters are set with $p_0 = 18$ and $T_0 = 20$.

5.2. *Model validation*

- **Social entity reputation.** The Reputation Factor serves as a reliable indicator for identifying malicious entities within the SIoE Network. Figure 6 illustrates the evolution of social entities in terms of their reputation over time. It depicts the temporal progression of feedback received by a provider, averaged over the total number of feedback instances. For the purpose of this evaluation, three social entity providers were randomly selected (specifically, the 5th, 6th, and 25th entity). In this scenario, only one of the selected entities exhibits malicious behavior by delivering poor services more frequently than the others. Consequently, the negative feedback directed toward this misbehaving entity adversely impacts its overall reputation. The results obtained from the SIoE simulator have been compared with those of the analytical model, ensuring that both methodologies processed an equal number of events. The marked curves in the figure represent the reputation trends of the entities as derived from the SIoE simulator, while the flat curves illustrate the trends obtained through the analytical model. Specifically, the reputation values have been calculated for each processed event by utilizing equation 12. Notably, the reputation values of social entities derived from the simulator demonstrate significant fluctuations during the initial processing of services. In contrast, the curves from the analytical model exhibit a much more stable trend. However, as the number of processed events increases, the discrepancies between the curves of the analytical model and the simulation diminish considerably, ultimately leading to convergence.

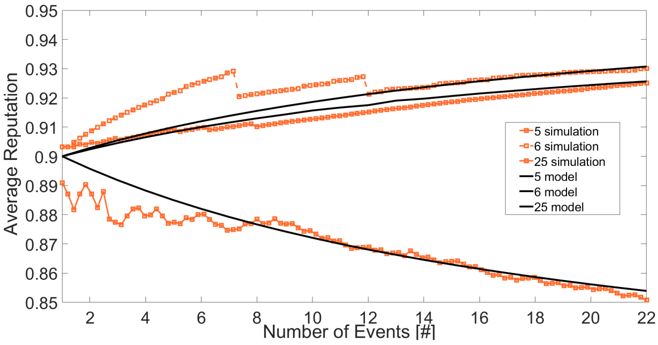


Figure 6: Average reputation validation.

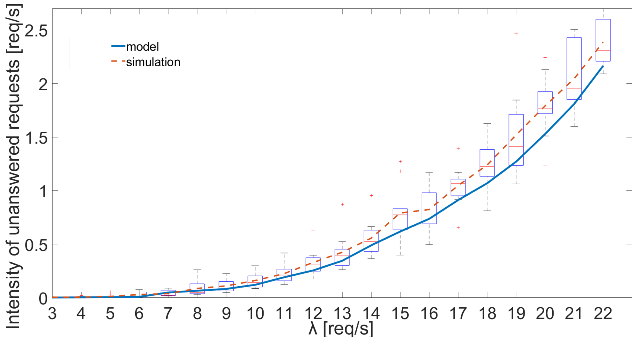
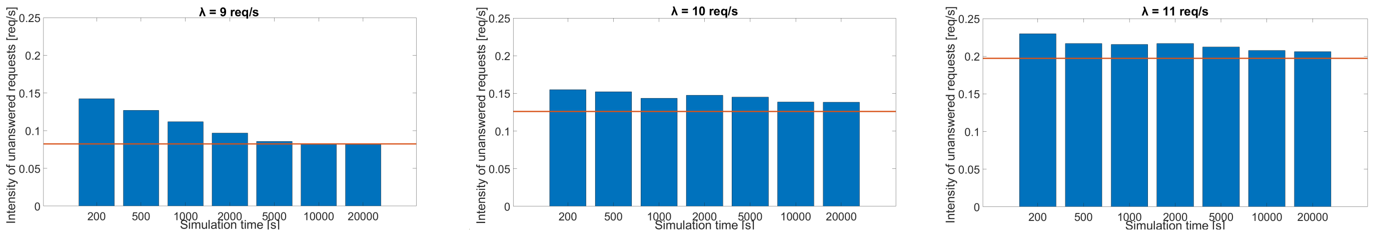


Figure 7: Intensity of unanswered request validation.

- **Resource availability in the cluster.** Another key performance indicator used for model validation is the intensity of unanswered requests in service provisioning. Figure 7 illustrates this indicator, showcasing the availability of a social entity as the traffic intensity λ increases. The model outcomes, obtained through the evaluation of equation 13, are represented by the continuous blue line. The simulated rate of unserved requests is depicted using box plot curves. In this representation, the central mark of each box denotes the median, while the bottom and top edges correspond to



(a) $\lambda = 9$

(b) $\lambda = 10$

(c) $\lambda = 11$

Figure 8: Simulation time convergence

the 25th and 75th percentiles, respectively. The marked curve illustrates the averaged trend. For low values of traffic requests (i.e., $\lambda \leq 12$), the variance of the values obtained from the simulator is notably low. Concurrently, the results from the analytical model align consistently with the simulator outcomes, as evidenced by the blue curve intersecting the median value of each box across all points. Conversely, at higher traffic request levels, the variation in the simulator outcomes becomes evident, resulting in wider boxes. Despite this significant variation, the analytical model continues to follow the same trend as the averaged outcomes from the simulator, further confirming the validity of the analytical results. Additionally, Figure 8 provides further insight into the convergence of steady-state results between the analytical model and the simulation presented in [29]. By considering fixed values of λ (specifically, $\lambda = 9, 10,$ and 11), it is shown that the proposed model immediately yields a value for the steady-state condition of unanswered traffic. In contrast, the bars related to [29] indicate that approximately 10,000 seconds (or about 3 hours) are required to achieve a steady-state result. This disparity highlights the extensive computational efforts and significant time commitment needed to evaluate steady-state results from the service provider selection process, particularly for SIoE systems with a large number of service requests and devices. This finding underscores the utility of the proposed analytical model, which effectively captures the long-term evolution of the overall service provisioning process. By ensuring system responsiveness and circumventing the need for extensive and continuous computational efforts, the model enhances the efficiency of service provisioning in social networks.

5.3. Numerical results

By leveraging the ability to estimate the behavior of a social entity, the proposed model can serve as an effective tool for establishing appropriate QoS thresholds in the context of service provisioning. Specifically:

- the maximum number of malicious entities so that the service can be successfully accomplished with a given probability (taken as design parameter);
- the minimum number of high-end providers (and their availability) to take the intensity of unanswered requests under a given limit (taken as design parameter).

The aforementioned thresholds will be determined based on various configuration scenarios, including global traffic intensity and the ratio of good to malicious service providers. Additionally, these thresholds can be effectively utilized to design the SIoE service community in terms of the number of service providers and their available resources, ensuring that service requests are successfully completed with a given probability, even in the presence of a certain number of malicious entities. In terms of reliability, the service community can be effectively configured to identify and exclude malicious entities from offering their resources for executing service requests. To achieve this, the analysis focuses on investigating the parameter $E[R_j|T_j]$, as detailed in Section 4, which represents the expected reputation of a social entity.

Table 4: Reputation analysis

Malicious Entities [%]	P_{pf} **for malicious entities**	**Community Reputation**	**Misbehaved Services [%]**
10	75	0.903	9.1
10	60	0.898	10.3
10	45	0.896	10.8
10	30	0.899	10.0
20	75	0.900	9.9
20	60	0.895	11.2
20	45	0.892	11.8
20	30	0.896	10.8
30	75	0.894	11.2
30	60	0.886	13.3
30	45	0.883	14.2
30	30	0.887	13.2
40	75	0.893	11.6
40	60	0.884	14.0
40	45	0.880	15.1
40	30	0.885	14.0

Table 4 provides an application example of the proposed model, demonstrating its utility in assessing the impact of malicious entities within a service community. The example is based on a real-world scenario from a Vehicular Social Network, as described in [7], where mobile nodes exhibit predictable social behavior. The model enables the evaluation of how the presence of malicious entities affects the overall service provisioning, offering insights into the reliability and trustworthiness of potential service providers.

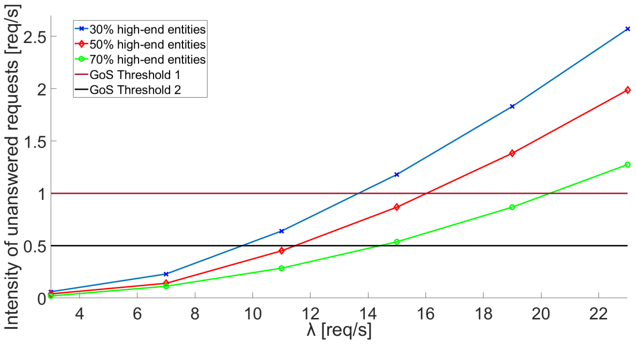


Figure 9: Unanswered requests analysis.

Table 5: Traffic requests analysis

λ [req/s]	High-end Entities [%]	Avg probability high-end availability	Intensity of unserved req. [req/s]
3	30	0.98	0.06
7	30	0.94	0.23
11	30	0.88	0.64
15	30	0.80	1.18
19	30	0.72	1.83
23	30	0.63	2.57
3	50	0.99	0.04
7	50	0.95	0.141
11	50	0.89	0.451
15	50	0.83	0.868
19	50	0.76	1.383
23	50	0.69	1.987
3	70	0.99	0.02
7	70	0.95	0.113
11	70	0.90	0.285
15	70	0.84	0.537
19	70	0.78	0.868
23	70	0.71	1.275

The steady-state percentage of misbehaved services is evaluated by examining various distributions of malicious entities, with the proportion ranging from 10% to 40% of the total entities involved in service provisioning. The second column of Table 4 displays the probability of receiving positive feedback for malicious entities, which quantifies the extent of their misbehavior. The overall community reputation is calculated by weighting the reputation of each entity within the service community based on the number of services provided by that entity. This is expressed by the following equation: $\sum_{j=1}^{N} E[R_j|T_j] \cdot \frac{T_j}{\Lambda}$, where Λ represents the total number of service requests processed by all providers. The results indicate that the percentage of misbehaved services increases with the proportion of malicious entities, and P_{pf} decreases. This trend highlights the potential hostile intentions of malicious providers. However, when the P_{pf} value for malicious entities drops significantly (e.g., $P_{pf} = 0.3$), these entities are no longer selected as service providers, resulting in a slight improvement in the overall network reputation. This demonstrates the model's ability to effectively capture the self-healing behavior of the SIoT trust management system.

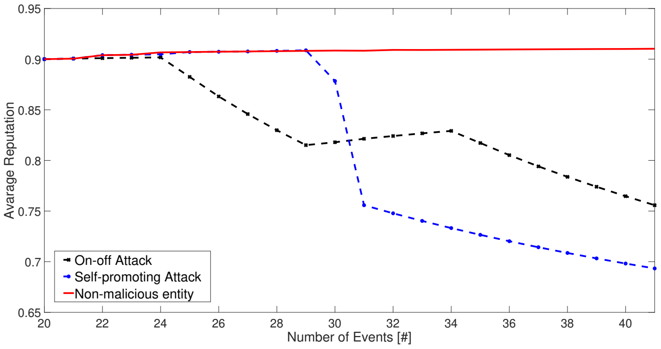


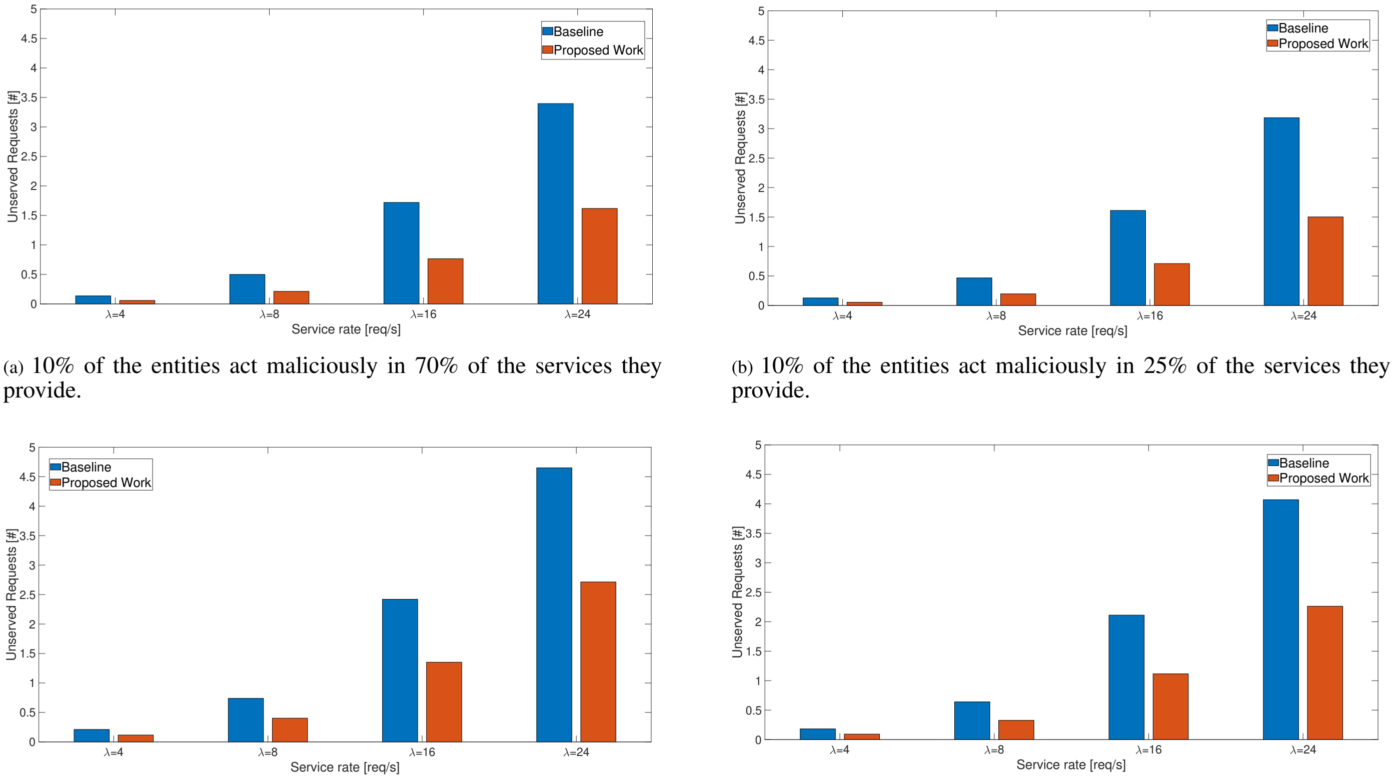
Figure 10: Analysis of well-known malicious attack on trust.

Similarly, the intensity of unanswered requests, $L(T_j)$, as formulated in Equation 13, can be utilized to establish the desired Grade of Service (GoS) for the SIoE cluster. This metric serves as a key indicator for estimating how many service requests can be successfully processed under the current network conditions. Evaluating $L(T_j)$ allows for the informed design and appropriate sizing of service communities by ensuring the allocation of social entities is aligned with their capacity to handle specific request loads. Table 5 presents the results for various configurations of service communities, characterized by differing percentages of high-end entities, ranging from 30% to 70%. The analysis is conducted under various traffic loads, with λ values ranging from 3 to 23 in increments of 4, and considers different average probabilities of service provider availability to accept service requests. It is evident that, for a constant percentage of high-end providers, an increase in λ results in a decrease in the average probability of availability among these providers, consequently leading to an increase in the intensity of unserved requests. It is crucial to highlight that the model can be effectively utilized to quantify the maximum traffic load that can be managed while achieving a specified minimum level of GoS, indicated by the maximum acceptable intensity of unanswered requests. This capability is further illustrated in Figure 9, which visually represents the results detailed in Table 5.

By establishing a GoS threshold, exemplified by the horizontal line in Figure 9, it becomes straightforward to determine the maximum value of λ for different percentages of high-end entities. This analysis clearly demonstrates which configurations of the SIoE network are capable of effectively processing a target request load.

5.4. *Malicious attack detection and baseline comparison*

An additional consideration regarding the Markov chain-based model for evaluating entity behavior within a SIoE environment is its capability to detect and assess specific reliability attacks targeting the system. In particular, the model fa-



(a) 10% of the entities act maliciously in 70% of the services they provide.

(b) 10% of the entities act maliciously in 25% of the services they provide.

(c) 25% of the entities act maliciously in 70% of the services they provide.

(d) 25% of the entities act maliciously in 25% of the services they provide.

Figure 11: Unserved requests comparison agains a baseline solution.

cilitates the identification of network entities exhibiting well-documented attack behaviors, enabling proactive mitigation and enhancing the overall trust and reliability of the network. The types of trust attacks analyzed in this work are comprehensively detailed in [35], including:

- On-Off Attack: a node periodically alternates its behavior between benevolent (ON) and malicious (OFF). During the ON phase, it builds up its trust, which is later exploited to attack the network during the OFF phase.

- Self-Promoting Attack: a malicious node provides positive recommendations about itself to increase its chances of being selected as a service provider. Once selected, it delivers poor or malicious services.

Such behaviors were identified by evaluating the average reputation of specific entities calculated in Section 4 and analyzing their state probabilities at a fixed steady-state step T_Δ. This approach enables a detailed examination of the entities' transition patterns, revealing deviations indicative of malicious behavior. Figure 10 presents three trends for comparison. The non-malicious entity (represented by the red curve) consistently performs the requested services at a nearly constant rate, resulting in a stable average reputation within the network. In contrast, the curves for entities detected as malicious exhibit typical patterns associated with the On-Off (black line) and Self-Promoting (blue line) attacks. In the On-Off attack, the entity alternates between increasing and decreasing its average reputation, strategically manipulating its standing to avoid a significant drop in the provider selection rankings. On the other hand, in the Self-Promoting attack, the node initially delivers services of the highest quality, maximizing its average reputation to secure selection as the preferred service provider. Once chosen, however, it begins delivering poor or malicious services.
Both attack patterns are recognized by the model through the evaluation of the entity's state, as indicated by the evolution of the probability of receiving positive feedback. This probability either increases or decreases depending on the type of attack affecting the network, significantly impacting the state probabilities. This allows the model to detect and potentially eliminate such malicious entities from the service provisioning process.

To further validate the applicability of the proposed model, this section presents a comparative analysis with a traditional trust management model from the current state of the art. The comparison focuses on the number of unserved requests at steady state, a critical metric for evaluating the efficiency of service provisioning in resource-constrained environments. Unlike the proposed model, the baseline approach does not explicitly incorporate resource availability into its state definition, which limits its ability to account for the dynamic capacity of service providers when selecting suitable entities for task fulfillment. Figure 11 illustrates the trend of unserved requests within the cluster across four distinct scenarios:

1. 10% malicious entities in the cluster, where malicious

nodes provide improper service with a probability of 70% and correct service with a probability of 30%.

2. 25% malicious entities in the cluster, where malicious nodes similarly provide improper service with a probability of 70% and correct service with a probability of 30%.

Each scenario highlights the impact of varying proportions of malicious entities and their behavior on the overall system performance in terms of unserved service requests. The evaluation considers four configurations, with service request rates progressively increasing from 4 requests per second (req/s) to 24 req/s. It is important to emphasize that unserved requests within the cluster result from the absence of a suitable provider capable of fulfilling the requested service. This may occur due to the following reasons: the provider offering the required service is malicious and either fails to deliver the service properly or does not participate in the service provider selection process, or the provider is temporarily unavailable due to insufficient resources to meet the service demand.

In general, a higher proportion of malicious nodes within the network (e.g., the scenario with 25% malicious entities) leads to a significant increase in the rate of unserved requests, primarily due to the reduction in trustworthy service providers.

Nevertheless, across all evaluated scenarios, the proposed model consistently outperforms the baseline by incorporating resource availability into the state probability calculations of the Markov chain. This integrated approach enhances the system's ability to identify suitable providers and allocate resources more efficiently.

The performance gap between the proposed model and the baseline becomes increasingly evident as the service request rate rises. For instance, at a high request rate of $\lambda = 24 req/s$, the proposed model demonstrates a reduction in the unserved request rate of up to 50% compared to the baseline, highlighting its robustness and scalability under high-demand conditions.

6. Conclusions

This paper presents a stochastic analytical model grounded in a multidimensional Markov chain framework for the selection of trusted providers in SIoE service provisioning. The proposed model effectively monitors the evolution of the reputation and capability of SIoE entities to fulfill service requests, while simultaneously filtering out malicious entities from the social network. Through validation and extensive testing, the analytical model has exhibited a substantial degree of convergence with simulation outcomes, operating within a computational complexity that is manageable for modern computing systems. This indicates its suitability and practicality for real-world SIoE scenarios. Numerical results testify that the model serves as an effective tool for detecting malicious behaviors, facilitating trustworthy operations, and enhancing overall system reliability.

Furthermore, the model can quantify the maximum traffic that the network can handle while still achieving a minimum GoS level in the service provisioning process. This capability is very helpful in guiding the design of the SIoE network structure, ensuring optimal performance under varying load conditions.

Appendix A. Details on the average number of requests assigned to a social entity

This Appendix elaborates on the derivation of Equation 5, as referenced in Section 3.1, which pertains to the calculation of λ_j. Specifically, this equation can be assessed by explicitly defining each possible value that the cardinality of ϕ may assume.

Assuming $|\phi| = 0$

By utilizing the joint probability distribution in accordance with the scheme $P(A|B,C) = \frac{P(A,B,C)}{P(B)}$, the probability $P(Req_{i\rightarrow j}|(p_j, T_j, c_j))$ can be expressed as follows:

$$P(Req_{i\rightarrow j}|(p_j, T_j, c_j)) = \frac{P(Req_{i\rightarrow j}, (p_j, T_j, c_j), |\phi| = 0)}{P(p_j, T_j, c_j)}. \quad \text{(A.1)}$$

Thus, transitioning from joint probability to conditional probability, we arrive at the following expression:

$$\begin{aligned} &P(Req_{i\rightarrow j}|(p_j, T_j, c_j)) = \\ &= \frac{P(Req_{i\rightarrow j}|((p_j, T_j, c_j), |\phi| = 0))P((p_j, T_j, c_j), |\phi| = 0)}{P(p_j, T_j, c_j)}. \end{aligned} \quad \text{(A.2)}$$

By applying Bayes' Theorem and simplifying the denominator, the previous equation can be reformulated as follows:

$$\begin{aligned} &P(Req_{i\rightarrow j}|(p_j, T_j, c_j)) = \\ &= \underbrace{P(Req_{i\rightarrow j}|((p_j, T_j, c_j), |\phi| = 0))}_{\Theta(|\phi|)} \cdot \underbrace{P(|\phi| = 0|(p_j, T_j, c_j))}_{\Omega(|\phi|)} \end{aligned} \quad \text{(A.3)}$$

where $\Theta(|\phi|)$ denotes the joint probability that a request from entity i is assigned to entity j, conditioned on the current state of j and the fact that no other social entities are considered more trustworthy than j by entity i. Conversely, $\Omega(|\phi|)$ represents the probability that no social entities exceed j in trustworthiness. Thus, assuming $|\phi| = 0$, there are no elements in $\mathcal{F}_i$ that are more trusted than j, the service request issued by entity i will be definitively assigned to entity j. Consequently, the probability defined by $\Theta(|\phi|)$ is equal to 1.

Let $n_1, n_2, j, \ldots, n_{|\mathcal{F}_i|}$ represent the friends of the social entity i belonging to the set $\mathcal{F}_i$. The assumption that there are no elements in $\mathcal{F}_i$ more trusted than j implies that the j-th social entity is the most trusted among them. Therefore, the probability $\Omega(|\phi|)$ can also be expressed as:

$$\begin{aligned} \Omega(|\phi|) = P(Tr_{ij} > Tr_{in_1}, &Tr_{ij} > Tr_{in_2}, ..., \\ &, ..., Tr_{ij} > Tr_{in_{|\mathcal{F}_i|}}|(p_j, T_j, c_j)). \end{aligned} \quad \text{(A.4)}$$

Assuming that these events are all independent of each other, it becomes:

$$\Omega(|\phi|) = \prod_{m=1}^{|\mathcal{F}_i|} P(Tr_{ij} > Tr_{in_m}|(p_j, T_j, c_j)) \tag{A.5}$$

Making explicit the Trust value, the previous equation can be also written as:

$$\Omega(|\phi|) = \prod_{m=1}^{|\mathcal{F}_i|} P(S_{ij}R_j > S_{in_m}R_{n_m}|(p_j, T_j, c_j)), \tag{A.6}$$

where S_{ij} and S_{in_m} represent the Sociality Factors estimating the degree of social relationship between the i-th entity and the j-th entity, as well as between the i-th entity and the n_m-th entity, respectively. Meanwhile, R_j and R_{n_m} denote the Reputation values of the j-th entity and the n_m-th entity, defined as:$R_j = \frac{p_j}{T_j}$ and $R_{n_m} = \frac{p_{n_m}}{T_{n_m}}$. Therefore,

$$\Omega(|\phi|) = \prod_{m=1}^{|\mathcal{F}_i|} P(p_{n_m} < \frac{S_{ij}R_jT_{n_m}}{S_{in_m}}) = \prod_{m=1}^{|\mathcal{F}_i|} \sum_{v=0}^{v_0} P(p_{n_m} = v) \tag{A.7}$$

where $v_0 = \left\lfloor \frac{S_{ij}R_jT_{n_m}}{S_{in_m}} \right\rfloor$. Developing the probability using the binomial distribution based on the Bernoulli process, we obtain:

$$\Omega(|\phi|) = \prod_{m=1}^{|\mathcal{F}_i|} \sum_{v=0}^{v_0} \binom{T_{n_m}}{v} \cdot P_{pf_{n_m}}^{v} \cdot (1 - P_{pf_{n_m}})^{T_{n_m}-v}, \tag{A.8}$$

where P_{pf_j} and $P_{pf_{n_m}}$ denote the probabilities that the j-th and n_m-th entities receive positive feedback following the provision of a service.

Finally, the average number of service requests assigned to the j-th social entity, denoted by λ_j, under the assumption that $|\phi| = 0$, can be expressed as shown in Equation A.9.

Assuming $|\phi| = 1$

The assumption of $|\phi| = 1$ can be articulated as the sum of the probabilities that precisely one entity within the set $\mathcal{F}_i$ is more trusted than the j-th provider, while no other entities share this status. Consequently, Equation 5 can be reformulated as presented in Equation A.10a. In this context, since all the stated events are mutually disjoint, the union can be extended across the entire equation. Consequently, the probability of the union of mutually disjoint events is equal to the sum of the probabilities of these events occurring, as shown in Equation A.10b. By employing the same methodology used to derive Equation A.3, Equation A.10b can subsequently be expressed as Equation A.10c.

For the sake of simplicity, we can analyze the two probabilities, denoted as $\Xi(\phi)$ and $\Psi(\phi)$, separately. In this context, the analysis of $\Xi(\phi)$ considers the scenario in which a service request from the i-th requester is assigned to the j-th service provider, even though the n_m-th entity, belonging to the set $\mathcal{F}_i$, may represent the most suitable candidate to execute the service. This choice can be rationalized by the unavailability of resources from the n_m-th most trusted service provider. In probabilistic terms, this unavailability can be conceptualized as the blocking probability associated with that entity, which is articulated in the following equation:

$$\begin{aligned} \Xi(|\phi|) &= P_B(n_m) = \\ &= \left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^{C_{n_m}} \frac{1}{C_{n_m}!} \frac{1}{\sum_{s=1}^{C_{n_m}} \left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^{s} \frac{1}{s!}}, \end{aligned} \tag{A.11}$$

where λ_{n_m} denotes the average number of service requests assigned to the n_m-th entity, μ_{n_m} signifies the average service rate utilized by the n_m-th entity to execute a service, and C_{n_m} represents the maximum amount of resources allocated by the n_m-th social entity.

The evaluation of $\Psi(|\phi|)$ involves calculating the probability that only one element of $\mathcal{F}_i$ is more trusted than the j-th provider, as articulated in the following equation:

$$\begin{aligned} \Psi(|\phi|) =& P(Tr_{in_1} \leq Tr_{ij}, Tr_{in_2} \leq Tr_{ij}, ..., \\ & , ..., Tr_{in_m} > Tr_{ij}, Tr_{in_{|\mathcal{F}_i|}} \leq Tr_{ij}|(p_j, T_j, c_j)). \end{aligned} \tag{A.12}$$

Assuming all events are independent and expliciting the Trust value, the previous equation can be expressed as follows:

$$\Psi(|\phi|) = P(S_{in_m}R_{n_m} > S_{ij}R_j) \prod_{l=1, l\neq m}^{|\mathcal{F}_i|} P(S_{in_l}R_{n_l} \leq S_{ij}R_j), \tag{A.13}$$

where R_j, R_{n_m}, and R_{n_l} denote the reputation values of the j-th, n_m-th, and n_l-th social entities, respectively. These values are calculated as: $R_j = \frac{p_j}{T_j}, \quad R_{n_m} = \frac{p_{n_m}}{T_{n_m}}, \quad R_{n_l} = \frac{p_{n_l}}{T_{n_l}}$.

Moreover, by setting and isolating the terms p_{n_m} and p_{n_l} as the random variables in the equation, we obtain:

$$\Psi(|\phi|) = \sum_{v=v_0+1}^{T_{n_m}} P(p_{n_m} = v) \prod_{l=1, l\neq m}^{|\mathcal{F}_i|} \sum_{v'=0}^{v_l} P(p_{n_l} = v') \tag{A.14}$$

where $v_0 = \left\lfloor \frac{S_{ij}R_jT_{n_m}}{S_{in_m}} \right\rfloor$ and $v_l = \left\lfloor \frac{S_{ij}R_jT_{n_l}}{S_{in_l}} \right\rfloor$.

By applying the binomial formula in a manner analogous to that used in Equation A.7, the probabilities $P(p_{n_m} = v)$ and $P(p_{n_l} = v')$ can be expressed as follows:

$$\begin{aligned} P(p_{n_m} = v) &= \binom{T_{n_m}}{v} \cdot (P_{pf_{n_m}})^{v} \cdot (1 - P_{pf_{n_m}})^{T_{n_m}-v}, \\ P(p_{n_l} = v') &= \binom{T_{n_l}}{v'} \cdot (P_{pf_{n_l}})^{v'} \cdot (1 - P_{pf_{n_l}})^{T_{n_l}-v'}, \end{aligned} \tag{A.15}$$

Finally, the average number of service requests assigned to the j-th social entity, denoted as λ_j, under the assumption that $|\phi| = 1$, can be expressed as shown in Equation A.16.

Assuming $|\phi| = 2$

$$\lambda_j(|\phi|=0) = \sum_{i=1}^{|\mathcal{F}_j|}\lambda_{ij}\prod_{m=1}^{|\mathcal{F}_i|}\sum_{\nu=0}^{\nu_0}\binom{T_{n_m}}{\nu}P^{\nu}_{pf_{n_m}}(1-P_{pf_{n_m}})^{T_{n_m}-\nu} \tag{A.9}$$

$$P(Req_{i\to j}|(p_j,T_j,c_j),|\phi|=1) = P(Req_{i\to j}|(p_j,T_j,c_j),\bigcup_{m=1}^{|\mathcal{F}_i|}(Tr_{in_m} > Tr_{ij}, \bigcap_{l=1,l\neq m}^{|\mathcal{F}_i|-1}(Tr_{in_l}\le Tr_{ij}))) = \tag{A.10a}$$

$$= \sum_{m=1}^{|\mathcal{F}_i|} P(Req_{i\to j}|(p_j,T_j,c_j), Tr_{in_m} > Tr_{ij}, \bigcap_{l=1,l\neq m}^{|\mathcal{F}_i|-1} Tr_{in_l}\le Tr_{ij}) = \tag{A.10b}$$

$$= \sum_{m=1}^{|\mathcal{F}_i|} \underbrace{P(Req_{i\to j}|((p_j,T_j,c_j), Tr_{in_m} > Tr_{ij}, \bigcap_{l=1,l\neq m}^{|\mathcal{F}_i|-1} P(Tr_{in_l}\le Tr_{ij})))}_{\Xi(|\phi|)} \cdot \underbrace{P(Tr_{in_m} > Tr_{ij}, \bigcap_{l=1,l\neq m}^{|\mathcal{F}_i|-1} Tr_{in_l}\le Tr_{ij}|(p_j,T_j,c_j))}_{\Psi(|\phi|)} \tag{A.10c}$$

$$\lambda_j(|\phi|=1) = \lambda_j(|\phi|=0) + \Big\{\sum_{i=1}^{|\mathcal{F}_j|}\lambda_{ij}\sum_{m=1}^{|\mathcal{F}_i|}\Big[\left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^{C_{n_m}}\frac{1}{C_{n_m}!}\frac{1}{\sum_{s=1}^{C_{n_m}}\left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^s\frac{1}{s!}}\cdot \\ \cdot\sum_{\nu=\nu_0+1}^{T_{n_m}}\binom{T_{n_m}}{\nu}(P_{pf_{n_m}})^{\nu}(1-P_{pf_{n_m}})^{T_{n_m}-\nu}\prod_{l=1,l\neq m}^{|\mathcal{F}_i|}\sum_{\nu'=0}^{\nu_l}\binom{T_{n_l}}{\nu'}(P_{pf_{n_l}})^{\nu'}(1-P_{pf_{n_l}})^{T_{n_l}-\nu'}\Big]\Big\} \tag{A.16}$$

The assumption of $|\phi = 2|$ can be articulated as the sum of the probabilities of all possible instances in which two entities from the set $\mathcal{F}_i$ are simultaneously more trusted than the provider j. Therefore, starting from equation 5, and following the same procedure outlined in the previous case, the probability $P(Req_{i\to j}|(p_j,T_j,c_j),|\phi|=2)$ can be expressed as shown in Equation A.17.

As in the previous case, the two probabilities $\Xi(|\phi|)$ and $\Psi(|\phi|)$ will be developed independently. Here, $\Xi(|\phi|)$ represents the event where a service request from the i-th service requester is assigned to the j-th provider, despite the presence of two other elements from the set $\mathcal{F}_i$ that are more trusted than j. This allocation occurs due to the lack of available resources exhibited by the n_m-th and n_z-th potentially most suitable service providers, which can be interpreted probabilistically as evaluating their blocking probabilities:

$$\begin{aligned}\Xi(|\phi|) =& P_B(n_m)\cdot P_B(n_z) = \\ &= \left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^{C_{n_m}}\frac{1}{C_{n_m}!}\frac{1}{\sum_{s=1}^{C_{n_m}}\left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^s\frac{1}{s!}}\cdot \\ &\cdot\left(\frac{\lambda_{n_z}}{\mu_{n_z}}\right)^{C_{n_z}}\frac{1}{C_{n_z}!}\frac{1}{\sum_{s=1}^{C_{n_z}}\left(\frac{\lambda_{n_z}}{\mu_{n_z}}\right)^s\frac{1}{s!}}.\end{aligned} \tag{A.18}$$

The evaluation of $\Psi(|\phi|)$, on the other hand, involves calculating the probability that the n_m-th and n_z-th entities, which belong to $\mathcal{F}_i$, are more trusted than the j-th provider. This can be expressed as follows:

$$\begin{aligned}\Psi(|\phi|) = P(&Tr_{in_1}\le Tr_{ij}, Tr_{in_2}\le Tr_{ij}, Tr_{in_m} > Tr_{ij}, ..., \\ &, ..., Tr_{in_z} > Tr_{ij}, Tr_{in_{|\mathcal{F}_i|}}\le Tr_{ij}|(p_j,T_j,c_j)).\end{aligned} \tag{A.20}$$

Assuming the independence of the events and making explicit the Trust values, the previous equation can be reformulated as follows:

$$\begin{aligned}\Psi(|\phi|) = &P(S_{in_m}\Delta_{n_m} > S_{ij}R_j)\cdot P(S_{in_z}R_{n_z} > S_{ij}R_j)\cdot \\ &\cdot\prod_{l=1,l\neq m,l\neq z}^{|\mathcal{F}_i|-2} P(S_{in_l}R_{n_l}\le S_{ij}R_j),\end{aligned} \tag{A.21}$$

where R_j, R_{n_m}, R_{n_z}, and R_{n_l} denote the Reputation factors of the j-th, n_m-th, n_z-th, and n_l-th social entities, respectively. These reputation values are defined as follows: $R_j = \frac{p_j}{T_j}$, $R_{n_m} = \frac{p_{n_m}}{T_{n_m}}$, $R_{n_z} = \frac{p_{n_z}}{T_{n_z}}$, $R_{n_l} = \frac{p_{n_l}}{T_{n_l}}$. Moreover, by isolating the terms p_{n_m}, p_{n_z}, and p_{n_l} as random variables, we can express the equation as follows:

$$P(Req_{i\to j}|(p_j,T_j,c_j),|\phi|=2)=\sum_{m=1}^{|\mathcal{F}_i|}\sum_{c=1,c\neq m}^{|\mathcal{F}_i|-1}\underbrace{P(Req_{i\to j}|((p_j,T_j,c_j),Tr_{in_m}>Tr_{ij},Tr_{in_c}>Tr_{ij},\prod_{l=1,l\neq m,l\neq z}^{|\mathcal{F}_i|-2}P(Tr_{in_l}\leq Tr_{ij})))}_{\Xi(|\phi|)}$$
$$\cdot\underbrace{P(Tr_{in_m}>Tr_{ij},Tr_{in_c}>Tr_{ij})\prod_{l=1,l\neq m,l\neq z}^{|\mathcal{F}_i|-2}P(Tr_{in_l}\leq Tr_{ij}|(p_j,T_j,c_j))}_{\Psi(|\phi|)} \qquad (A.17)$$

$$\lambda_j(|\phi|=2)=\lambda_j(|\phi|=0)+\lambda_j(|\phi|=1)+\sum_{i=1,i\neq j}^{|\mathcal{F}_j|}\lambda_{ij}\cdot\Big\{\sum_{m=1}^{|\mathcal{F}_i|}\sum_{z=1,z\neq m}^{|\mathcal{F}_i|-1}\Big[\left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^{C_{n_m}}\frac{1}{C_{n_m}!}\frac{1}{\sum_{s=1}^{C_{n_m}}\left(\frac{\lambda_{n_m}}{\mu_{n_m}}\right)^s\frac{1}{s!}}\cdot$$
$$\cdot\left(\frac{\lambda_{n_z}}{\mu_{n_z}}\right)^{C_{n_z}}\frac{1}{C_{n_z}!}\frac{1}{\sum_{s=1}^{C_{n_z}}\left(\frac{\lambda_{n_z}}{\mu_{n_z}}\right)^s\frac{1}{s!}}\sum_{\nu=\nu_0+1}^{T_{n_m}}\binom{T_{n_m}}{\nu}P^{\nu}_{pf_{n_m}}(1-P_{pf_{n_m}})^{T_{n_m}-\nu}\cdot$$
$$\cdot\sum_{\nu'=\nu_z+1}^{T_{n_z}}\binom{T_{n_z}}{\nu'}P^{\nu'}_{pf_{n_z}}(1-P_{pf_{n_z}})^{T_{n_z}-\nu'}\prod_{l=1,l\neq m}^{|\mathcal{F}_i|-2}\sum_{\nu''=0}^{\nu_l}\binom{T_{n_l}}{\nu''}P^{\nu''}_{pf_{n_l}}(1-P_{pf_{n_l}})^{T_{n_l}-\nu''}\Big]\Big\}. \qquad (A.19)$$

$$\Psi(|\phi|)=\sum_{\nu=\nu_0+1}^{T_{n_m}}P(p_{n_m}=\nu)\cdot\sum_{\nu'=\nu_z+1}^{T_{n_z}}P(p_{n_z}=\nu')\cdot$$
$$\cdot\prod_{l=1,l\neq m}^{|\mathcal{F}_i|-2}\sum_{\nu''=0}^{\nu_l}P(p_{n_l}=\nu''), \qquad (A.22)$$

where $\nu_0=\lfloor\frac{S_{ij}R_jT_{n_m}}{S_{in_m}}\rfloor$, $\nu_z=\lfloor\frac{S_{ij}R_jT_{n_z}}{S_{in_z}}\rfloor$, and $\nu_l=\lfloor\frac{S_{ij}R_jT_{n_l}}{S_{in_l}}\rfloor$.

By employing a binomial formula analogous to the one used in equation (A.7), the probabilities $P(p_{n_m}=\nu)$, $P(p_{n_z}=\nu')$, and $P(p_{n_l}=\nu'')$ can be computed as follows:

$$P(p_{n_m}=\nu)=\binom{T_{n_m}}{\nu}\cdot P^{\nu}_{pf_{n_m}}\cdot(1-P_{pf_{n_m}})^{T_{n_m}-\nu},$$
$$P(p_{n_z}=\nu')=\binom{T_{n_z}}{\nu'}\cdot P^{\nu'}_{pf_{n_z}}\cdot(1-P_{pf_{n_z}})^{T_{n_z}-\nu'}, \qquad (A.23)$$
$$P(p_{n_l}=\nu'')=\binom{T_{n_l}}{\nu''}\cdot P^{\nu''}_{pf_{n_l}}\cdot(1-P_{pf_{n_l}})^{T_{n_l}-\nu''},$$

Finally, the average number of service requests assigned to the j-th social entity, denoted by λ_j, assuming $|\phi|=2$, can be expressed as as reported in the Equation A.19.

Assuming $|\phi|$ be greater than 2

It is worth noting that the formula A.17 can be extended to cases where $|\phi|=3$, $|\phi|=4$, and so forth, i.e., scenarios in which three, four, or more entities are more trusted than j, but all lack available resources. However, the probability of such events becomes negligible when compared to the cases considered, and thus they are not included as further contributions in Equation 5. In fact, evaluating the probability in Equation A.17 for higher values of $|\phi|$ would lead to excessive model complexity, with only a marginal improvement in accuracy.

Appendix B. Computational complexity of the average number of requests assigned to a social entity

Assuming that the probability of events where $|\phi|$ exceeds 2 is negligible, the evaluation of the complexity of the λ_j term simplifies to the sum of the elementary operations performed in Equations A.9, A.16, and A.19.

$$N_\lambda=|\mathcal{F}_j|\Big[\Big[(|\mathcal{F}_i|)(\nu_0+1)\Big]+$$
$$+\Big[(|\mathcal{F}_i|)(C_{n_m}+T_{n_m}-\nu_0+(|\mathcal{F}_i|)(\nu_l+1))\Big]+$$
$$+\Big[(|\mathcal{F}_i|)(|\mathcal{F}_i|-1)(C_{n_m}+C_{n_z}+T_{n_m}-\nu_0+T_{n_z}-$$
$$+\nu_z+(|\mathcal{F}_i|-2)(\nu_l+1))\Big]\Big]. \qquad (B.1)$$

Considering the cardinality of the sets of friends of the entities as expressed in the model's development, we now investigate the upper bound of the term N_λ. Assuming that the quantities $T_{n_m}\simeq T_{n_z}$ and $\nu_0\simeq\nu_z\simeq\nu_l$, given that they correspond to social entities presumed to be of the same type, the equation for N_λ (Equation B.1) simplifies to the following expression:

$$N_\lambda<|\mathcal{F}_j|\Big[|\mathcal{F}_i|\nu_0+|\mathcal{F}_i|C_{n_m}+|\mathcal{F}_i|T_{n_m}-|\mathcal{F}_i|\nu_0+$$
$$+|\mathcal{F}_i|^2\nu_0+\Big[|\mathcal{F}_i|^2C_{n_m}+|\mathcal{F}_i|^2C_{n_m}+2|\mathcal{F}_i|^2T_{n_m}- \qquad (B.2)$$
$$+2|\mathcal{F}_i|^2\nu_0+|\mathcal{F}_i|^3\nu_0\Big]\Big].$$

Furthermore, by design, the term expressing the maximum amount of resources for an entity, denoted as C_{n_m}, is significantly smaller than the other quantities involved in the model (e.g., $C_{n_m} \ll T_{n_m}$ or $C_{n_m} \ll |\mathcal{F}_i|$). As a result, this term becomes negligible when determining the overall order of complexity of λ_j. Assuming the term T_{n_m} as the step that characterizes the steady-state of the Markov chain, as calculated in equation 14, we obtain:

$$
\begin{aligned}
N_\lambda < |\mathcal{F}_j|\Big[|\mathcal{F}_i|T_\Delta + 2|\mathcal{F}_i|^2 T_\Delta - |\mathcal{F}_i|^2 \nu_0 + |\mathcal{F}_i|^3 \nu_0\Big] = \\
= |\mathcal{F}_i|^3|\mathcal{F}_j|\nu_0 + |\mathcal{F}_i|^2|\mathcal{F}_j|(2T_\Delta - \nu_0) + |\mathcal{F}_i||\mathcal{F}_j|T_\Delta.
\end{aligned}
\tag{B.3}
$$

Revealing that the order of complexity for calculating λ_j is $O(|\mathcal{F}_i|^3|\mathcal{F}_j|\nu_0)$, this shows that the computational complexity increases cubically with the cardinality of the set $\mathcal{F}_i$.

Acknowledgements

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, in the context of partnership on “Telecommunications of the Future” (PE00000001 - program “RESTART”, CUP: D93C22000910001), national center on “Sustainable Mobility” (CN00000023 - program “MOST”, CUP: D93C22000410001), and partnership on “Cybersecurity” (PE00000007 - program “SERICS”, CUP: D33C22001300002, project ISP5G+). It was also supported by the PRIN 2022 projects INSPIRE (grant no. 2022BEXMXN_01) and HORUS (grant no. 2022P44KA8) funded by the Italian MUR, by the HORIZON MSCA project BRIDGITISE (grant no. 101119554) and the HORIZON JU SNS project 6G-GOALS (grant no. 101139232), and by “The house of emerging technologies of Matera (CTEMT)” project funded by the Italian MIMIT.

References

[1] S. Murtuza, Internet of everything: Application and various challenges analysis a survey, in: 2022 1st International Conference on Informatics (ICI), 2022, pp. 250–252. doi:10.1109/ICI53355.2022.9786891.

[2] A. J. Chinchawade, O. S. Lamba, Authentication schemes and security issues in internet of everything (ioe) systems, in: 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 342–345. doi:10.1109/CICN49253.2020.9242569.

[3] L. Atzori, A. Iera, G. Morabito, From ”smart objects” to ”social objects”: The next evolutionary step of the internet of things, IEEE Communications Magazine 52 (1) (2014) 97–105. doi:10.1109/MCOM.2014.6710070.

[4] L. Atzori, A. Iera, G. Morabito, M. Nitti, The social internet of things (siot) – when social networks meet the internet of things: Concept, architecture and network characterization, Computer Networks 56 (16) (2012) 3594–3608. doi:https://doi.org/10.1016/j.comnet.2012.07.010.
URL https://www.sciencedirect.com/science/article/pii/S1389128612002654

[5] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, K.-S. Kwak, The internet of things for health care: A comprehensive survey, IEEE Access 3 (2015) 678–708. doi:10.1109/ACCESS.2015.2437951.

[6] K. M. Alam, M. Saini, A. E. Saddik, Toward social internet of vehicles: Concept, architecture, and applications, IEEE Access 3 (2015) 343–357. doi:10.1109/ACCESS.2015.2416657.

[7] A. M. Vegni, C. Leoni, V. Loscri, A. Benslimane, A reputation-based trustworthiness concept for wireless networking in vehicular social networks, IEEE Communications Magazine (2023) 1–7doi:10.1109/MCOM.001.2300249.

[8] A. Kirimtat, O. Krejcar, A. Kertesz, M. F. Tasgetiren, Future trends and current state of smart city concepts: A survey, IEEE Access 8 (2020) 86448–86467. doi:10.1109/ACCESS.2020.2992441.

[9] M. Fadda, M. Anedda, R. Girau, G. Pau, D. D. Giusto, A social internet of things smart city solution for traffic and pollution monitoring in cagliari, IEEE Internet of Things Journal 10 (3) (2023) 2373–2390. doi:10.1109/JIOT.2022.3211093.

[10] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, Q. Arshad, When social objects collaborate: Concepts, processing elements, attacks and challenges, Computers and Electrical Engineering 58 (2017) 397–411. doi:https://doi.org/10.1016/j.compeleceng.2016.11.014.

[11] C.-H. Hsu, C. E. Montenegro Marin, R. Gonzalez Crespo, H. F. Mohamed El-sayed, Guest editorial introduction to the special section on social computing and social internet of things, IEEE Transactions on Network Science and Engineering 9 (3) (2022) 947–949. doi:10.1109/TNSE.2022.3167460.

[12] V. Sharma, I. You, D. N. K. Jayakody, M. Atiquzzaman, Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social internet of things, Future Generation Computer Systems 92 (2019) 758–776. doi:https://doi.org/10.1016/j.future.2017.12.039.

[13] M. Nitti, L. Atzori, I. P. Cvijikj, Friendship selection in the social internet of things: Challenges and possible strategies, IEEE Internet of Things Journal 2 (3) (2015) 240–247. doi:10.1109/JIOT.2014.2384734.

[14] L. Wei, J. Wu, C. Long, B. Li, On designing context-aware trust model and service delegation for social internet of things, IEEE Internet of Things Journal 8 (6) (2021) 4775–4787. doi:10.1109/JIOT.2020.3028380.

[15] C. Boudagdigue, A. Benslimane, A. Kobbane, M. Elmachkour, A distributed advanced analytical trust model for iot, in: 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1–6. doi:10.1109/ICC.2018.8422726.

[16] G. Joshi, V. Sharma, Light-weight hidden markov trust evaluation model for iot network, in: 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 142–149. doi:10.1109/I-SMAC52330.2021.9640885.

[17] E. Wang, C. Chen, D. Zhao, W. Ip, K. Yung, A dynamic trust model in internet of things, Soft Computing 24 (8) (2020) 5773–5782. doi:10.1007/s00500-019-04319-2.

[18] Y. Chen, M. Zhou, Z. Zheng, D. Chen, Time-aware smart object recommendation in social internet of things, IEEE Internet of Things Journal 7 (3) (2020) 2014–2027. doi:10.1109/JIOT.2019.2960822.

[19] Z. U. Shamszaman, M. I. Ali, Toward a smart society through semantic virtual-object enabled real-time management framework in the social internet of things, IEEE Internet of Things Journal 5 (4) (2018) 2572–2579. doi:10.1109/JIOT.2017.2779106.

[20] A. Souri, Y. Zhao, M. Gao, A. Mohammadian, J. Shen, E. Al-Masri, A trust-aware and authentication-based collaborative method for resource management of cloud-edge computing in social internet of things, IEEE Transactions on Computational Social Systems (2023) 1–10doi:10.1109/TCSS.2023.3241020.

[21] S. Zhang, D. Zhang, Y. Wu, H. Zhong, Service recommendation model based on trust and qos for social internet of things, IEEE Transactions on Services Computing 16 (5) (2023) 3736–3750. doi:10.1109/TSC.2023.3274647.

[22] S. Sagar, A. Mahmood, K. Wang, Q. Z. Sheng, J. K. Pabani, W. E. Zhang, Trust–siot: Toward trustworthy object classification in the social internet of things, IEEE Transactions on Network and Service Management 20 (2) (2023) 1210–1223. doi:10.1109/TNSM.2023.3247831.

[23] W. Tan, Y. Wang, L. Liu, W. Xiaoding, T. Ding, Adaptive federated deep learning-based semantic communication in the social internet of things, IEEE Internet of Things Journal PP (2024) 1–1. doi:10.1109/JIOT.2024.3484230.

[24] B. Allakaram Tawfeeq, A. Masoud Rahmani, A. Koochari, N. Jafari Navimipour, An improved evolutionary method for social internet of things

service provisioning based on community detection, IEEE Access 12 (2024) 132939–132963. doi:10.1109/ACCESS.2024.3457672.

[25] C. Fu, Q. Li, M. Shen, K. Xu, Frequency domain feature based robust malicious traffic detection, IEEE/ACM Transactions on Networking 31 (1) (2023) 452–467. doi:10.1109/TNET.2022.3195871.

[26] R. Faqihi, D. Ramakrishnan, D. Mavaluru, An evolutionary study on the threats, trust, security, and challenges in siot (social internet of things), Materials today: proceedings (11 2020). doi:10.1016/j.matpr.2020.09.618.

[27] B. Farahbakhsh, A. Fanian, M. H. Manshaei, TGSM: Towards trustworthy group-based service management for social IoT, Internet of Things 13 (2021) 100312. doi:https://doi.org/10.1016/j.iot.2020.100312.

[28] G. Sciddurlo, I. Huso, D. Striccoli, G. Piro, G. Boggia, A multi-tiered social iot architecture for scalable and trusted service provisioning, in: 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1–6. doi:10.1109/GLOBECOM46510.2021.9685084.

[29] G. Sciddurlo, A. Petrosino, D. Striccoli, G. Piro, L. A. Grieco, G. Boggia, Boosting service provisioning in siot by exploiting trust and capability levels of social objects, in: 2022 IEEE International Conference on Smart Computing (SMARTCOMP), 2022, pp. 1–6. doi:10.1109/SMARTCOMP55677.2022.00077.

[30] W. Z. Khan, Q. u. A. Arshad, S. Hakak, M. K. Khan, Saeed-Ur-Rehman, Trust management in social internet of things: Architectures, recent advancements and future challenges, IEEE Internet of Things Journal (2020) 1–1doi:10.1109/JIOT.2020.3039296.

[31] C. Marche, I. Cabiddu, C. G. Castangia, L. Serreli, M. Nitti, Implementation of a multi-approach fake news detector and of a trust management model for news sources, IEEE Transactions on Services Computing 16 (6) (2023) 4288–4301. doi:10.1109/TSC.2023.3311629.

[32] F. de Trizio, G. Sciddurlo, A. Petrosino, G. Piro, G. Boggia, A scalable framework for responsive trustworthiness dissemination in social ioa, in: Proceedings of the CoNEXT Student Workshop 2024 (CoNEXT-SW '24), December 9–12, 2024, Los Angeles, CA, USA, CoNEXT-SW '24, Association for Computing Machinery, Los Angeles, California, 2024. doi:10.1145/3694812.3699925.

[33] G.Fink, Markov models for pattern recognition: from theory to applications, no. 248 in XII, Springer, 2014. doi:https://doi.org/10.1007/978-3-540-71770-6.

[34] M. O. Ojo, S. Giordano, G. Procissi, I. N. Seitanidis, A review of low-end, middle-end, and high-end iot devices, IEEE Access 6 (2018) 70528–70554. doi:10.1109/ACCESS.2018.2879615.

[35] C. Marche, M. Nitti, Trust-related attacks and their detection: A trust management model for the social iot, IEEE Transactions on Network and Service Management 18 (3) (2021) 3297–3308. doi:10.1109/TNSM.2020.3046906.