A Review of Game Theory-Based Trust Modeling Approaches in Infrastructure-Free Social Networks

Alireza Seddighi[1], SeyyedAmir Asghari[2*], Morteza Romoozi[3], Hamideh Babaei[4]

1. PhD student, Department of Computer Engineering, Qom Branch, Islamic Azad University, Qom, Iran.
2. Associate Professor, Department of Electrical and Computer Engineering, Kharazmi University, Tehran, Iran.
3. Assistant Professor, Department of Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran.
4. Assistant Professor, Department of Computer Engineering, Narag Branch, Islamic Azad University, Narag, Iran.

*** Corresponding author email address**: asghari@khu.ac.ir

Received: 2024-12-05 **Reviewed:** 2025-01-03 **Revised:** 2025-01-21 **Accepted:** 2025-02-03 **Published:** 2025-04-14

Abstract

This study aims to review and classify game theory-based trust modeling approaches in infrastructure-free social networks, highlighting their mechanisms, applications, and limitations. A narrative review methodology with a descriptive analysis approach was employed to examine peer-reviewed literature published between 2015 and 2025. The review focused on trust modeling strategies within infrastructure-free networks such as MANETs, VANETs, DTNs, and UAV/IoT systems. Game-theoretic models were categorized into non-cooperative, cooperative, evolutionary, and Bayesian/repeated frameworks. Relevant articles were identified through targeted searches in leading academic databases using defined inclusion criteria. The models were compared based on theoretical assumptions, game mechanisms, trust evaluation metrics, scalability, computational overhead, and security resilience. Non-cooperative models prioritize individual rationality and minimal overhead but struggle against strategic deception. Cooperative models emphasize coalition formation and fairness in resource sharing, offering improved trust propagation at the cost of increased communication. Evolutionary approaches enable adaptation and learning through repeated interactions but require longer convergence times. Repeated and Bayesian games facilitate historical learning and probabilistic trust estimation, showing strong potential in dynamic and uncertain environments. Across all types, trade-offs were observed between robustness, scalability, and complexity. Key challenges identified include computational cost, dynamic topology, vulnerability to collusion, and limited real-world deployment. The integration of AI, privacy-preserving mechanisms, and cross-layer modeling remains underexplored but promising. Game theory offers a versatile and strategic foundation for trust modeling in decentralized, infrastructure-free networks. While existing models address various trust challenges effectively, further research is needed to enhance scalability, incorporate intelligent adaptation, and ensure practical deployment in real-world applications. The future lies in hybrid, context-aware, and privacy-focused trust systems that combine the strengths of game-theoretic reasoning with emerging technologies.

Keywords: *Game theory, trust modeling, infrastructure-free networks.*

How to cite this article:

Seddighi, A., Asghari, S.A., Romoozi, M., Babaei, H. (2025). Presenting the Management Accounting Model in the Digital Era. Management Strategies and Engineering Sciences, 7(4), 81-95.

1. Introduction

Infrastructure-free social networks, encompassing systems such as Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), and Delay-Tolerant Networks (DTNs), represent a dynamic class of decentralized communication environments characterized by their lack of fixed infrastructure. Unlike traditional networks, where data transmission is managed through centralized routers or base stations, these networks are entirely self-organizing. In MANETs, for instance, each node operates as both a host and a router, allowing communication to be maintained without centralized control, even in highly mobile or remote contexts. VANETs build on similar principles but are specifically designed for vehicular environments, facilitating vehicle-to-vehicle and vehicle-to-infrastructure communications with the goal of enhancing road safety and traffic efficiency. DTNs, on the other hand, are tailored to environments where network connectivity is intermittent or highly variable, employing a store-and-forward approach to ensure message delivery over time despite frequent disconnections or long delays [1, 2]. These infrastructure-free social networks have proven to be vital in scenarios ranging from disaster recovery and military operations to intelligent transportation systems and rural connectivity solutions, where traditional communication infrastructure may be unavailable or unreliable [3, 4].

Despite their versatility and potential, infrastructure-free social networks are fundamentally challenged by their decentralized nature, particularly when it comes to establishing and maintaining trust among nodes. The lack of a central authority means that each node must rely on its own judgment to determine the reliability of others, making trust management a crucial component for secure and efficient communication. In environments such as VANETs, where vehicles exchange critical safety information, or DTNs, where messages may traverse through multiple unknown intermediaries, ensuring the trustworthiness of data sources and relay nodes is essential to prevent data corruption, misinformation, or malicious interference [5, 6]. Without trust mechanisms, malicious entities could easily exploit the system by misrouting packets, injecting false information, or simply refusing to forward data, leading to network fragmentation and reduced performance [7, 8]. Trust, therefore, becomes not only a measure of security but also a fundamental enabler of cooperation, data integrity, and network resilience in these distributed systems.

In recent years, the modeling of trust in decentralized systems has evolved beyond simple reputation-based or rule-based approaches to more strategic and adaptive frameworks, with game theory emerging as a particularly powerful tool. Game theory, rooted in mathematics and economics, provides a formal framework to model the interactions between rational agents who may have competing interests or incomplete information about one another. In the context of infrastructure-free networks, game theory allows for the design of trust models that account for the strategic behavior of nodes, including incentives for cooperation, punishment for defection, and mechanisms for reputation building over time [9, 10]. For instance, in MANETs, non-cooperative game models can simulate scenarios where nodes must decide whether to forward packets based on expected rewards or penalties, thereby mimicking real-world dilemmas such as the prisoner's dilemma or the trust game [11, 12].

Moreover, the versatility of game-theoretic approaches allows them to be adapted to various network contexts. Cooperative games, for example, are often used in VANETs to encourage coalition formation among vehicles that can jointly maximize network performance while ensuring mutual trust [13]. Evolutionary game theory has also been leveraged in DTNs and other dynamic environments, enabling nodes to adapt their trust strategies based on previous interactions and observed outcomes, thus reflecting the learning processes observed in biological or social systems [14, 15]. The application of Bayesian games further enhances trust modeling by accounting for uncertainties in node behavior, allowing trust to be inferred probabilistically based on past actions and limited information [16, 17]. These game-theoretic strategies collectively provide a robust and scalable means of simulating and managing trust in highly dynamic and decentralized settings, where traditional security measures often fall short.

The objective of this review is to explore and synthesize the range of game theory-based trust modeling approaches developed for infrastructure-free social networks. By examining how different game-theoretic models have been applied to address trust in MANETs, VANETs, DTNs, and similar contexts, this paper aims to highlight the strengths and limitations of these strategies, categorize them based on their underlying game frameworks, and identify emerging trends and research gaps. Given the increasing reliance on decentralized networks in both civilian and critical applications, a comprehensive understanding of trust modeling through the lens of game theory is essential for designing secure, reliable, and adaptive communication systems. Through a descriptive analysis of literature from 2015 to 2025, this article contributes to the growing discourse on how strategic decision-making frameworks can enhance the trustworthiness and performance of infrastructure-free social networks.

2. Methodology

This narrative review employed a descriptive analysis approach to systematically explore and synthesize the body of literature on game theory-based trust modeling approaches within infrastructure-free social networks. The descriptive analysis method was selected due to its suitability for mapping complex and interdisciplinary subjects that span multiple research domains, including network security, distributed systems, and applied game theory. Rather than statistically aggregating results, this method allows for a comprehensive examination of conceptual frameworks, methodologies, and applications, focusing on trends, themes, and variations across studies. The review was designed to provide an in-depth understanding of the evolution, strengths, and limitations of game-theoretic trust models in the context of networks lacking centralized infrastructure, including mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), delay-tolerant networks (DTNs), and related environments.

The literature search was conducted using a comprehensive and systematic strategy across multiple academic databases including IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink, Scopus, and Google Scholar. Search terms were formulated using combinations of keywords such as "game theory," "trust model," "trust evaluation," "trust management," "infrastructure-free networks," "ad hoc networks," "vehicular networks," and "delay-tolerant networks." Boolean operators were applied to refine the search scope and ensure relevance, using queries like ("game theory" AND "trust" AND "infrastructure-free" OR "ad hoc") and similar formulations. The search was restricted to peer-reviewed journal articles, conference proceedings, and high-quality review papers published between 2015 and 2025, ensuring that the analysis focused on the most recent and impactful developments in the field. Duplicate studies were removed, and initial screening was performed based on titles and abstracts to identify articles that specifically addressed the integration of game theory in trust modeling for decentralized or infrastructure-free network environments.

Following the initial screening, full-text articles were reviewed to confirm their relevance and to extract detailed information on the theoretical models, game-theoretic mechanisms, trust metrics, simulation tools, and application domains. Studies were included if they explicitly applied game-theoretic principles—such as cooperative games, non-cooperative games, repeated games, evolutionary games, or Bayesian games—to trust modeling in infrastructure-free network environments. Studies that used other trust mechanisms without game-theoretic foundations or that were not situated within decentralized network contexts were excluded. A qualitative data extraction process was employed, focusing on the structural components of each trust model, its assumptions, the type of game used, the environment simulated or targeted, and the performance evaluation methods and outcomes. Thematic analysis was conducted to classify models into major categories based on the type of game theory applied and the nature of their application domain. This classification formed the basis for comparative evaluation and the identification of research trends and gaps presented in the later sections of this review.

3. Classification of Game-Theoretic Trust Models

Game theory has proven to be a foundational tool in designing trust mechanisms within infrastructure-free social networks. These networks, due to their lack of centralized oversight, demand decentralized yet strategic trust models that can operate under uncertain conditions and resist malicious behavior. Game-theoretic trust models are typically categorized into non-cooperative, cooperative, evolutionary, repeated, and Bayesian frameworks. Each type captures distinct assumptions about node behavior, interaction dynamics, and strategic decision-making. This section offers a descriptive classification of these models based on their design principles and applications, outlining the assumptions behind each approach and analyzing their strengths and limitations.

3.1. Non-Cooperative Game-Based Models

Non-cooperative game models are among the earliest and most frequently applied approaches in trust modeling for infrastructure-free networks. These models assume that each node acts independently and rationally, aiming to maximize its own utility without forming binding agreements with others. The primary assumption in non-cooperative games is that nodes may be selfish, and their trustworthiness is evaluated based on observable behaviors, such as willingness to forward packets or share resources. These models typically simulate scenarios where cooperation is not guaranteed unless incentivized through rewards or deterrents.

An example of a non-cooperative trust model can be found in the work by Wang et al., who designed a trust measurement model based on a two-player game where each node evaluates the risk and benefit of trusting another node in a social network setting [17]. Similarly, Li and colleagues presented a model that employs strategic interactions among agents in decentralized environments to decide whether to cooperate or defect based on payoffs, providing a formal mechanism to quantify trust in social networks [11]. These models are particularly well-suited for mobile ad hoc networks (MANETs) where the high mobility of nodes and absence of central control demand localized and real-time decision-making.

Non-cooperative models are praised for their simplicity and direct application to realistic selfish behaviors often observed in open networks. However, their limitations become apparent when dealing with sophisticated adversaries or colluding nodes. Without cooperative incentives, these models may result in unstable trust decisions or fail to sustain long-term cooperation. Moreover, the assumption of rationality may not hold true in networks involving heterogeneous agents with varying capabilities or goals. As noted by Chen et al., non-cooperative models may be insufficient in complex trust environments where adaptive or historical behavior must be considered [12].

3.2. *Cooperative Game-Based Models*

Unlike non-cooperative models, cooperative game-based models assume that nodes can form coalitions to achieve mutually beneficial outcomes. These models are grounded in the belief that collaboration among trusted nodes can enhance network performance and improve security, especially in situations where group-based routing or resource sharing is required. Cooperative games are particularly suitable for vehicular networks (VANETs), where vehicles can coordinate their actions for traffic efficiency and safety.

Ravale et al. presented a cooperative approach to trust management that leverages the principles of game theory to encourage collaboration among network nodes. In their model, trust is reinforced through coalition formation, and nodes are rewarded proportionally based on their contributions to network reliability and security [13]. This mechanism helps ensure fairness, discourage free-riding, and improve system-wide trust propagation. Similarly, Bai and colleagues introduced a cooperative game framework focused on energy efficiency and emission reduction in wireless communication networks, where nodes form strategic groups to optimize power usage while maintaining trust relationships [4].

Coalition formation introduces benefits that are often absent in non-cooperative models, such as stability in trust relations and the possibility of long-term collaboration. The principles of fairness and rationality are central to cooperative games, especially in reward-sharing schemes. For instance, solutions like the Shapley value or core allocations are often used to distribute rewards fairly among participants based on their marginal contributions. However, implementing cooperative models in practice poses challenges, particularly in terms of overhead and coalition negotiation. The dynamic topology of infrastructure-free networks can hinder stable group formation, and misreporting or strategic manipulation by malicious nodes may still threaten the integrity of coalitions [6, 8].

3.3. *Evolutionary Game Theory Approaches*

Evolutionary game theory offers a dynamic and adaptive framework for trust modeling, diverging from the classical assumption of fixed rationality. Instead of presuming that agents make decisions based on full knowledge of the environment, evolutionary models simulate how strategies evolve over time through repeated interactions and adaptation. This approach is particularly advantageous in infrastructure-free networks like delay-tolerant networks (DTNs), where node behavior changes frequently due to environmental variability, intermittent connectivity, and resource constraints.

A noteworthy application of evolutionary game theory is provided by Dhakal et al., who explored cooperation and trust evolution in an N-player social dilemma game using migration tags. Their study demonstrates how cooperative behavior can emerge and persist in decentralized environments when nodes adapt their strategies based on social cues and contextual information [14]. Similarly, Zhang et al. applied evolutionary game theory to study safety supervision among construction workers in complex networks, modeling how safety compliance evolves through local interactions and trust feedback [15]. These studies highlight the flexibility of evolutionary models to capture emergent phenomena in trust dynamics.

The strength of evolutionary approaches lies in their ability to incorporate learning and adaptation. Nodes can modify their trust assessments based on past experiences, leading to strategies that reflect real-world uncertainties and behavioral diversity. Moreover, evolutionary models can accommodate noise and mutation, allowing for the occasional deviation from optimal strategies, which is often observed in human and agent-based systems [18, 19]. However, evolutionary models also face limitations. Convergence to stable strategies can be slow, and the outcomes depend heavily on initial conditions and selection mechanisms. Additionally, ensuring convergence to desirable equilibrium states in highly mobile or adversarial networks remains an open challenge.

3.4. Repeated and Bayesian Games in Trust Evaluation

Repeated games and Bayesian games represent another significant category of trust models that rely on historical interaction and probabilistic reasoning. In repeated games, trust is built through a series of interactions where nodes remember past behavior and adjust their strategies accordingly. This setting is suitable for environments where nodes encounter each other multiple times over the network lifetime, enabling reputation systems and punishment strategies to enforce cooperation.

Razin and Feigh introduced a model of repeated interactions to explain how trust develops in human-robot collaboration, arguing that commitment to interdependence over time can sustain trust even in the presence of uncertainty [20]. Repeated game frameworks are also used in MANETs to encourage consistent behavior, where defecting nodes face long-term consequences such as exclusion from data forwarding. These models rely heavily on memory mechanisms and discounting of past actions to weigh current trust decisions.

Bayesian games, by contrast, are specifically designed to handle incomplete information. In these models, nodes do not have full visibility into the types or intentions of others but maintain beliefs that are updated over time based on observed behavior. Bayesian games provide a rigorous method for modeling trust under uncertainty, particularly when trust must be inferred from indirect observations or noisy feedback. Nojoumian’s rational trust modeling framework incorporates Bayesian reasoning to dynamically adjust trust values based on both direct and indirect interactions, demonstrating how belief systems can be encoded within strategic decision-making [16].

Repeated and Bayesian game models excel in representing realistic trust scenarios where agents must account for uncertainty, past performance, and strategic deception. They support the development of robust reputation systems and allow for trust recovery after temporary misbehavior, offering flexibility in dynamic and error-prone environments. However, these models can be computationally intensive, especially in large networks where maintaining and updating belief systems requires substantial resources [21, 22]. Furthermore, designing appropriate incentive structures and belief update rules remains a complex task, particularly when nodes possess heterogeneous risk preferences or act maliciously.

In summary, the classification of game-theoretic trust models highlights the richness and diversity of approaches developed to enhance trust in infrastructure-free social networks. Non-cooperative models emphasize individual strategy and self-interest, cooperative models focus on collaboration and fairness, evolutionary models simulate adaptation over time, and repeated and Bayesian games provide mechanisms for historical learning and probabilistic reasoning. Each approach addresses different facets of trust and is suited to specific network conditions, offering a multi-dimensional toolkit for managing trust in decentralized and infrastructure-less environments.

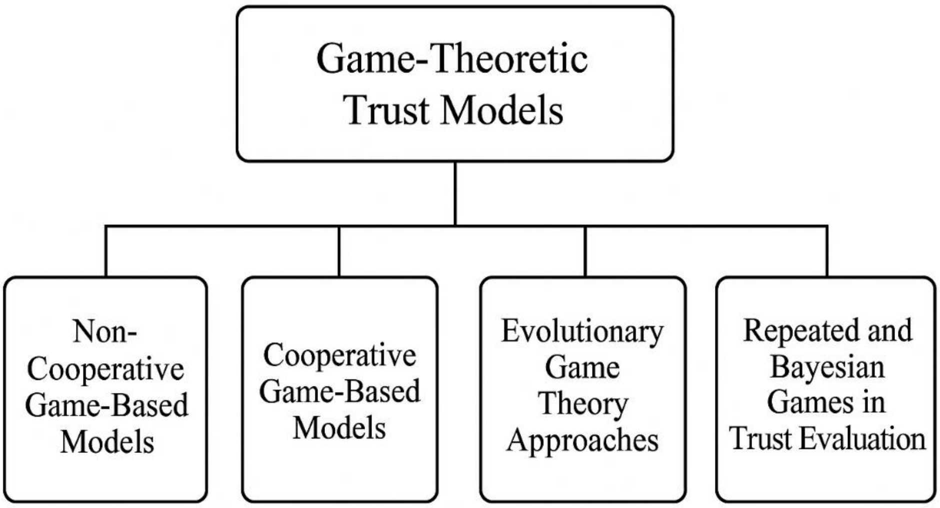
Game-Theoretic Trust Models
Non-Cooperative Game-Based Models
Cooperative Game-Based Models
Evolutionary Game Theory Approaches
Repeated and Bayesian Games in Trust Evaluation

Figure 1. Game-Theoretic Trust Models

4. Application Domains

The application of game theory-based trust models across various infrastructure-free networks has marked a significant advancement in secure and efficient communication. Each domain—whether mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), delay-tolerant networks (DTNs), or UAV and IoT edge environments—presents unique challenges that influence the structure, implementation, and evaluation of trust models. Game-theoretic mechanisms provide a strategic and adaptive approach to managing trust where centralized control is absent and nodes must continuously assess the reliability of their peers under dynamic conditions. In each of these application settings, the choice of game-theoretic model is typically guided by specific environmental constraints, communication protocols, and behavioral assumptions about nodes or agents.

4.1. Mobile Ad Hoc Networks (MANETs)

In mobile ad hoc networks, nodes are free to move independently and form spontaneous network topologies. Trust modeling in MANETs is crucial due to the network's decentralized architecture and the vulnerability of nodes to misbehavior, selfishness, and resource depletion. Game theory offers a structured framework for addressing these vulnerabilities by modeling node interactions as strategic decisions aimed at maximizing utility while maintaining overall network performance.

Non-cooperative game theory has been widely applied in MANETs to analyze the behavior of autonomous nodes that may choose to cooperate or defect in forwarding packets. For instance, Wang et al. developed a game-theoretic trust measurement model tailored for social networks but equally applicable to MANET scenarios, where each node independently assesses the expected payoff of interacting with another node based on observed behaviors and local trust values [17]. The lack of a centralized entity makes this model particularly suitable for MANETs, where each node must make autonomous trust evaluations in real-time. Similarly, Li and Li introduced a trust valuation model based on non-cooperative game theory, allowing nodes to dynamically adjust their trust levels based on the outcomes of prior interactions [11]. Their model emphasizes local computation and strategic foresight, reflecting the adaptive nature of trust in highly mobile environments.

In addition to non-cooperative games, cooperative strategies have been introduced to foster long-term collaboration. Bai et al. proposed a self-organizing game-theoretic approach where nodes work together to reduce energy consumption, addressing one of the primary concerns in MANETs: limited battery life and computational capacity [4]. This cooperative framework encourages packet forwarding and reduces selfish behavior by ensuring that nodes share network benefits based on their level of participation. Such reward-based trust reinforcement models have demonstrated the ability to balance individual rationality and collective benefit, promoting more sustainable network behavior.

Repeated games and evolutionary game theory have also found extensive use in MANETs. The dynamic topology of these networks lends itself to models that incorporate memory and learning. Chen et al. designed a model where nodes evolve their strategies over time based on the historical outcomes of trust interactions, thereby enhancing resilience against random or malicious misbehavior [12]. This model incorporates probabilistic learning and decision-making, reflecting real-world uncertainties in wireless environments. Moreover, evolutionary models such as the one explored by Dhakal et al. simulate adaptation mechanisms in large-scale MANETs, where node behavior changes in response to shifting environmental and social cues [14]. These adaptive models provide nuanced insights into the emergence of trust and cooperation under real-world constraints, including node heterogeneity and intermittent connectivity.

4.2. *Vehicular Ad Hoc Networks (VANETs)*

VANETs represent a unique infrastructure-free environment characterized by high node mobility, predictable movement patterns, and critical timing requirements. In such networks, vehicles communicate with each other (V2V) and with roadside units (V2I) to share traffic updates, safety alerts, and other time-sensitive information. Trust in VANETs is especially critical, as malicious behavior or misinformation can lead to safety hazards and cascading traffic issues.

Game-theoretic trust models in VANETs often incorporate elements of coalition formation, where vehicles collaborate to ensure secure and efficient message dissemination. Ravale et al. proposed a trust management model based on cooperative game theory, where vehicles form strategic alliances to share traffic data and reward one another for honest behavior [13]. This approach not only ensures data integrity but also supports fairness in resource allocation, as rewards are distributed based on each vehicle's contribution. These coalition-based mechanisms are well-suited to the high-density and fast-paced nature of vehicular environments, where trust decisions must be made quickly and accurately.

In some VANET settings, trust models rely on repeated interactions to identify consistent patterns of trustworthy or untrustworthy behavior. Razin and Feigh highlighted how repeated game dynamics can be used to simulate interactions between vehicles and autonomous systems, reinforcing cooperation over time through mechanisms like tit-for-tat or reputation decay [20]. This method allows the network to adaptively penalize malicious nodes and reward those with sustained positive behavior, thereby enhancing long-term network reliability.

Bayesian games have also been applied in VANET contexts to manage trust under uncertainty. Given that vehicles may not always have direct communication with others, they often rely on indirect observations or inferred behavior. Nojoumian’s Bayesian-based trust framework supports this inference mechanism by updating trust levels using probabilistic reasoning, thereby offering a flexible and context-aware model for decision-making [16]. This approach is particularly useful in dense urban areas where vehicles interact with a large and frequently changing set of peers.

A critical concern in VANET trust modeling is ensuring scalability and robustness against collusion. Al-Zahrani and Thomas investigated the impact of trust models on routing protocols under attack conditions, showing that trust-based enhancements to the AODV protocol can significantly reduce vulnerability to flooding and other forms of misinformation [8]. Game theory in this context serves as both a predictive and defensive mechanism, enabling networks to preempt and respond to strategic adversarial behaviors.

4.3. *Delay-Tolerant Networks (DTNs)*

Delay-tolerant networks are designed for environments with intermittent connectivity, long latency, and frequent partitions. These characteristics are common in remote geographic regions, deep-space communication, and post-disaster recovery scenarios. Trust modeling in DTNs is particularly challenging because nodes may never interact directly, and messages are often stored and forwarded across long time spans. Consequently, game-theoretic trust models in DTNs must account for sparse communication, asynchronous interactions, and indirect observation of behavior.

Evolutionary game theory is particularly well-suited to DTNs due to its ability to simulate long-term strategy adaptation. Dhakal et al. demonstrated how nodes in DTNs evolve cooperative behaviors through repeated interactions and social tagging, allowing trust to emerge organically in the absence of continuous feedback [14]. These models reflect the gradual nature of trust development in sparse networks and support decision-making even with limited interaction histories.

Bayesian trust models are also essential in DTNs, where incomplete information and uncertain outcomes are the norm. Li et al. proposed a data-driven evolutionary game model that incorporates trust inference in heterogeneous environments, making it applicable to DTNs where direct trust data is unavailable [19]. By simulating trust propagation through probabilistic beliefs, the model enhances delivery efficiency and data integrity in conditions where message routing depends on opportunistic encounters.

Trust-based routing has been a focal point of game-theoretic applications in DTNs. Grandi et al. addressed the strategic disclosure of information in delay-sensitive settings by modeling how nodes selectively share or withhold data based on trust levels and perceived utility [6]. Such models enable nodes to prioritize trustworthy peers and reduce the risk of data loss or corruption during extended delays.

A further challenge in DTNs is balancing energy consumption and security. Tolkachov et al. explored how trust-aware game-theoretic strategies can optimize traffic segmentation and resource allocation in distributed networks, providing a framework that supports energy-efficient routing and protects against trust-based attacks [18]. Their model underscores the importance of combining trust evaluation with physical network constraints, making it particularly relevant for DTNs deployed in resource-limited environments.

4.4. UAV and IoT Edge Environments

The integration of unmanned aerial vehicles (UAVs) and edge-based Internet of Things (IoT) devices has given rise to a new class of infrastructure-free networks with unique trust challenges. UAV networks are characterized by high mobility, constrained energy, and critical mission objectives, while IoT edge environments often involve heterogeneous devices, intermittent connectivity, and sensitive data.

In UAV networks, game theory has been applied to ensure mission cooperation and data reliability. Mssassi and Kalam introduced a game-theoretic incentive model designed for blockchain-based UAV networks, aiming to mitigate malicious behavior and encourage data sharing through rational incentives [21]. Their model combines elements of non-cooperative and cooperative games to balance individual and collective goals in a distributed aerial system.

In the context of IoT edge computing, game theory supports both trust evaluation and load balancing. Wang et al. investigated how different dimensions of trust, such as competence and morality, influence the acceptance of smart infrastructure projects in edge-enabled networks [23]. Their findings highlight the need for multi-faceted trust models that integrate behavioral insights and strategic interaction, particularly in public-facing IoT applications.

Bayesian inference and repeated games are frequently used in these environments to monitor device behavior over time and infer trustworthiness under uncertain conditions. For example, Kejriwal simulated inequality in strategic agent networks, offering a model where resource distribution and node reputation evolve through interactions in decentralized IoT ecosystems [5]. These simulations are instrumental in understanding how trust disparities emerge and persist in edge environments.

The complexity of IoT networks often necessitates cross-layer trust models. Thanappan and Perumal proposed a congestion-aware routing protocol based on evolutionary game theory, demonstrating how nodes can adapt to network stress while maintaining trust relationships [24]. This integration of network performance and trust dynamics is crucial for edge environments where latency and reliability are critical.

Collectively, the application of game theory-based trust models across MANETs, VANETs, DTNs, and UAV/IoT environments illustrates the adaptability and strategic depth of game-theoretic frameworks. These models offer tailored solutions to the distinct challenges of each domain, enabling decentralized networks to foster cooperation, resist malicious behavior, and adapt to environmental uncertainties through rational and context-aware trust mechanisms.

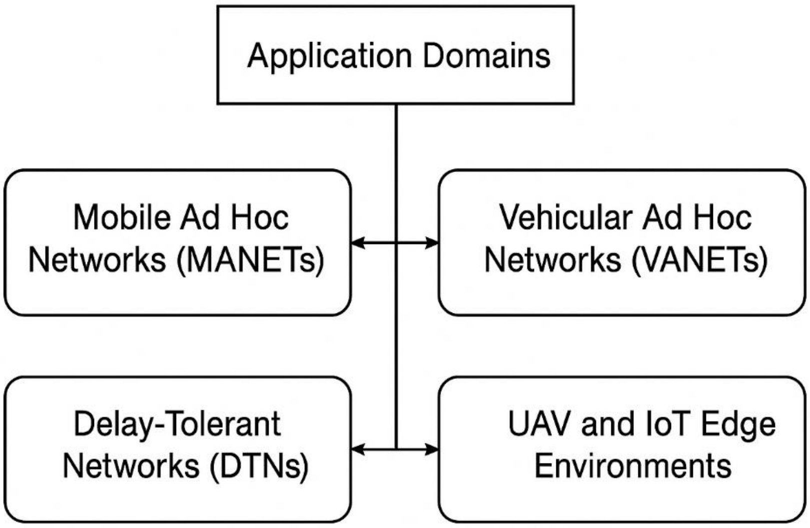
Application Domains
Mobile Ad Hoc Networks (MANETs)
Vehicular Ad Hoc Networks (VANETs)
Delay-Tolerant Networks (DTNs)
UAV and IoT Edge Environments

Figure 2. Application Domains

5. Comparative Analysis of Existing Models

The landscape of game theory-based trust modeling in infrastructure-free social networks is marked by a rich diversity of approaches, each designed to address specific network demands, behavioral assumptions, and threat landscapes. In synthesizing the key features of these models, it becomes evident that their comparative effectiveness depends heavily on the theoretical foundations employed, the mechanisms of trust measurement and updating, and the trade-offs they manage between computational efficiency and robustness against malicious behaviors. Using a descriptive analysis approach, this section provides a comparative view of the major model types, trust evaluation strategies, scalability features, and security capacities within the current literature.

When analyzing model types and assumptions, a distinct divergence emerges between non-cooperative and cooperative frameworks. Non-cooperative game-theoretic trust models typically assume that nodes act independently and rationally to maximize individual utility, without any binding commitment to cooperate. In the model proposed by Wang et al., trust is calculated using a payoff matrix that simulates the outcomes of strategic choices made by each node in forwarding or rejecting packets within the network [10]. This model reflects the assumption that each node operates in isolation and selects its strategies based on observed benefits, without any central coordination. In contrast, cooperative models like those developed by Ravale et al. introduce the possibility of coalition formation, assuming that nodes may coordinate their behaviors to achieve mutual benefit [13]. Such models inherently presume a degree of inter-node communication and trust willingness that extends beyond the logic of pure self-interest.

A third perspective is introduced through evolutionary game theory, which abandons the static assumptions of rationality and instead models how trust behaviors emerge and evolve over time. In the evolutionary framework introduced by Dhakal et al., nodes are allowed to adapt their strategies based on the success of previous interactions and social cues such as tagging, which reflect behavioral traits rather than strict payoff values [14]. This model presumes that nodes do not always make optimal decisions and may experiment or mutate strategies, leading to a more organic evolution of trust in dynamic environments. On the other hand, Bayesian game-based models assume that nodes operate under incomplete information and adjust their beliefs based on observed actions. In Nojoumian's model, trust is probabilistically inferred using Bayesian updating rules that incorporate both direct experience and third-party recommendations, making it particularly relevant for networks where interactions are sporadic and information is partial or indirect [16].

The choice of game-theoretic mechanism directly impacts the robustness and flexibility of trust evaluation. Static games such as the prisoner's dilemma or trust games are foundational to many non-cooperative models, including the one by Li and Li, where the core idea is to represent the interaction between two nodes as a binary decision of cooperation or defection [11]. These models are computationally simple and suitable for real-time decisions in low-resource environments, but they often fail to capture the complexity of long-term relationships or repeated encounters. In contrast, models like those by Razin and Feigh utilize repeated games to simulate ongoing interactions where trust is shaped through consistency over time and where strategies such as tit-for-tat encourage cooperative behavior by responding to defection with punishment in future rounds [20]. Repeated games provide a stronger foundation for trust accumulation in networks like VANETs or UAV systems, where the same nodes may interact repeatedly.

Bayesian games offer another nuanced mechanism, as seen in the work by Chen et al., who use probabilistic reasoning to predict trustworthiness based on a node's history and indirect observations [22]. These models are highly flexible and context-sensitive but require considerable computational resources for belief management and updating. Cooperative mechanisms often integrate solutions like the Shapley value or Nash bargaining solutions to ensure fair reward distribution among coalition members. For example, in the cooperative game approach by Bai et al., the allocation of energy-saving benefits among network nodes is calculated based on their marginal contributions to the coalition, thus encouraging participation while avoiding exploitation [4]. These mechanisms introduce additional overhead but significantly enhance fairness and cooperation incentives.

Trust metrics and update strategies are central to the operationalization of any trust model. In many non-cooperative models, trust is quantified through direct interaction outcomes, using simple additive or multiplicative formulas to increase or decrease trust scores. For example, in the model proposed by Wang et al., trust updates are based on success or failure in packet delivery and are adjusted incrementally in real-time [17]. While efficient, these models are vulnerable to false positives and negatives in rapidly changing environments. Cooperative and Bayesian models often employ more sophisticated update strategies, incorporating weighted averages of peer recommendations, historical consistency, and context variables. Nojoumian's model, for example, updates trust by integrating Bayesian inference with rational expectations, where each piece of evidence adjusts the posterior belief in a node's reliability [16].

Evolutionary models differ in that they often use fitness functions rather than discrete trust scores. In the model by Zhang et al., strategies evolve based on their relative success, and trust emerges from the prevalence of cooperative behavior within the population over time [15]. These models support learning and adaptation but may require many iterations to stabilize, making them less suitable for time-sensitive applications. Additionally, models that integrate blockchain infrastructure, such as the one by Mssassi and Kalam, use decentralized ledgers to record and verify trust evaluations, ensuring tamper-resistance and transparency in trust propagation [21]. However, these systems introduce significant computational and communication overhead, which may not be viable for low-power or bandwidth-constrained networks.

Scalability and overhead are major differentiators among trust models, especially in large-scale networks such as IoT edge systems or vehicular networks. Non-cooperative models, due to their minimal reliance on global knowledge or communication, scale relatively well. In Erturkoglu et al.'s study of mobile social game platforms, a non-cooperative trust mechanism allowed users to dynamically assess the reliability of services without requiring centralized servers or heavy messaging protocols [25]. However, the drawback of scalability in such models lies in their limited contextual awareness and vulnerability to fragmentation when trust values become isolated or overly localized.

Cooperative models, such as those proposed by Ravale et al., often incur higher communication and processing overhead due to the need for coalition negotiation, contribution tracking, and reward distribution [13]. This is particularly evident in environments like VANETs, where maintaining real-time coalitions in high-mobility scenarios can overwhelm system resources. Similarly, Bayesian models can become resource-intensive as the number of potential node types increases, requiring each node to maintain and update a growing belief matrix. In highly dynamic networks like DTNs, as shown in the work of Tolkachov et al., segmentation and trust-based routing strategies were introduced to reduce overall overhead while maintaining effective trust propagation [18].

Evolutionary models present a middle ground by enabling local adaptation with limited global communication. In Dhakal et al.'s evolutionary trust model, nodes update strategies based on local interactions and migration patterns, reducing the need for centralized data exchange while maintaining dynamic responsiveness [14]. However, convergence to optimal strategies may require extended periods of simulation or real-time operation, potentially delaying the realization of full trust stabilization.

Security resilience remains a critical comparative dimension, particularly with regard to selfish or malicious nodes. Non-cooperative models are generally more vulnerable to strategic deception, especially in the absence of punitive mechanisms. In Wang et al.'s model, a lack of long-term memory or punishment allows malicious nodes to exploit the trust of cooperative peers by appearing honest in isolated interactions [10]. Repeated games address this gap by introducing reputational memory and retaliation strategies. The model by Razin and Feigh exemplifies how mutual monitoring and memory of past actions can deter betrayal and reinforce cooperative behavior over time [1].

Cooperative models can also be undermined by collusion or Sybil attacks unless trust evaluation includes mechanisms for cross-validation and redundancy. In response to these concerns, Al-Zahrani and Thomas implemented a trust-based AODV routing protocol capable of detecting and isolating flooding attackers, demonstrating how game-theoretic trust metrics can be embedded into security-aware routing decisions [8]. Evolutionary models, while robust to gradual deception, may be slow to react to sudden shifts in node behavior. Their reliance on trend-based adaptation means that malicious strategies may proliferate before being recognized and countered. On the other hand, Bayesian models, as implemented in the work of Chen et al., are well-suited to environments with partial or noisy data, where traditional rule-based approaches may fail. These models offer probabilistic resilience by continuously adjusting belief distributions and discounting outliers, thereby filtering deceptive behaviors over time [22].

Overall, the comparative analysis of existing game-theoretic trust models reveals that no single model excels across all evaluation dimensions. Non-cooperative games are computationally efficient but limited in security robustness. Cooperative models offer rich interaction dynamics and fairness but suffer from higher overhead. Evolutionary frameworks provide adaptive and decentralized learning but require longer convergence. Bayesian models excel in uncertain and incomplete information environments but demand greater computational effort. Ultimately, the suitability of any trust model depends on the network's scale, mobility, resource availability, and threat profile. Hybrid approaches that combine elements of these models—such as integrating repeated game logic into Bayesian inference or applying evolutionary adaptation within cooperative coalitions—may offer a more comprehensive solution for the trust challenges in modern infrastructure-free social networks.

6. Challenges and Research Gaps

While game theory-based trust modeling in infrastructure-free social networks has made considerable strides, several critical challenges and research gaps remain that impede its widespread adoption and effectiveness. These issues relate not only to theoretical limitations but also to practical constraints such as computational efficiency, adaptability to dynamic environments, resistance to coordinated malicious behavior, and applicability in real-world settings. A careful examination of these challenges reveals the pressing need for further refinement and innovation in model design, deployment strategies, and interdisciplinary integration.

Scalability and computational cost remain persistent obstacles, particularly as trust models are deployed in large-scale and resource-constrained networks such as Internet of Things (IoT) systems or vehicular ad hoc networks. Many game-theoretic models, especially those using Bayesian or cooperative frameworks, demand significant memory, processing, and communication resources. For example, in the model by Nojoumian, trust is updated through Bayesian inference, requiring the continuous adjustment of belief states and prior probabilities based on observed behavior and recommendations from peers [16]. While this approach provides high accuracy in trust estimation, it becomes increasingly burdensome as the number of nodes and interactions grows. Similarly, cooperative models like those developed by Bai et al., which depend on the calculation of marginal contributions and equitable reward distributions, require centralized or semi-centralized coordination that may not be feasible in environments with limited bandwidth or processing capabilities [4]. The evolutionary models proposed by Dhakal et al., although decentralized and adaptive, also face scaling limitations due to the slow convergence of strategies and the requirement for repeated interactions across many agents [14].

A second major challenge is the handling of malicious collusion and coordinated adversarial strategies. Most trust models are designed to detect and punish isolated misbehavior; however, they often struggle against nodes that collude to manipulate trust metrics or launch Sybil attacks. In cooperative frameworks, where nodes share trust values and resources, colluding nodes can artificially boost each other's reputations, undermining the reliability of the trust assessment. Al-Zahrani and Thomas explored this issue in the context of AODV routing under flooding attacks, illustrating how the manipulation of trust data can degrade network performance and compromise security [8]. Similarly, Ravale et al. emphasized that without robust countermeasures, coalition-based trust schemes can be easily infiltrated by adversaries posing as cooperative nodes [13]. Despite these risks, relatively few models implement explicit defenses against collusion, highlighting a critical gap in existing research.

The dynamic topology and mobility of nodes in infrastructure-free networks further complicate trust evaluation. In MANETs and VANETs, nodes frequently enter and exit communication ranges, and trust decisions must be made rapidly and often with incomplete information. Models such as the one proposed by Wang et al., which rely on accumulated direct interaction history, may not perform effectively when interactions are infrequent or short-lived [17]. Furthermore, trust mechanisms that assume relatively stable social relationships or repeated encounters may fail in highly transient environments. The repeated game model introduced by Razin and Feigh is particularly sensitive to such dynamics, as it assumes that nodes will engage in ongoing interactions that allow for punishment and reward strategies to influence behavior over time [1]. In highly mobile networks, the opportunity for repeated interactions is often limited, reducing the effectiveness of such trust enforcement mechanisms.

Another significant challenge lies in integrating game-theoretic trust models with artificial intelligence (AI)-based trust prediction and decision-making systems. While AI offers powerful tools for behavior analysis, anomaly detection, and adaptive learning, it remains underutilized in most existing game-theoretic models. The work by Chen et al., which leverages neuroimaging and behavioral data to understand trust propensity, highlights the potential of combining cognitive modeling with AI to enhance trust evaluation in human-agent networks [22]. However, the integration of such methods with game-theoretic logic remains in its infancy. Bridging these methodologies could lead to more nuanced and predictive trust systems, yet research exploring this convergence is limited.

Finally, a widespread limitation across current literature is the lack of real-world deployment and empirical validation of game theory-based trust models. Most models are tested in simulated environments or small-scale testbeds, which may not accurately reflect the complexities and unpredictability of real-world networks. For instance, the Bayesian model by Nojoumian and the evolutionary models by Zhang et al. demonstrate impressive theoretical performance but lack large-scale empirical data supporting their claims [15]. As Tolkachov et al. noted in their analysis of corporate network segmentation, the transition from simulation to deployment requires addressing real-world issues such as noisy data, device heterogeneity, and user unpredictability [18]. Without field trials and cross-validation, the scalability, robustness, and practicality of these models remain uncertain, presenting a barrier to their adoption in mission-critical applications like emergency response or autonomous vehicular coordination.

7. Future Research Directions

To address the current challenges and advance the field, several promising research directions can be pursued. One critical avenue involves the development of hybrid models that combine the strategic rigor of game theory with the predictive capabilities of machine learning. These models could dynamically adjust game parameters, such as payoff values or cooperation thresholds, based on real-time behavioral analytics or anomaly detection systems. The work by Kejriwal, which models inequality in agent networks, hints at the benefits of simulation-informed strategic adaptation, and integrating such frameworks with reinforcement learning algorithms could enable nodes to autonomously refine their trust strategies in complex, data-rich environments [5]. Hybrid approaches can leverage historical patterns detected by AI to fine-tune game-theoretic strategies, enabling more proactive and context-sensitive trust management.

A second important direction is the design of context-aware and lightweight trust mechanisms. Many current models are computationally intensive or require detailed network knowledge, which may not be feasible in low-resource settings. Future research should focus on streamlining trust calculations using heuristics, probabilistic shortcuts, or edge-computing strategies, allowing deployment on constrained devices such as IoT sensors or UAVs. The model by Wang et al., which addresses the moral and ability dimensions of trust, suggests that incorporating situational variables into trust assessments can significantly enhance decision accuracy while reducing complexity [23]. Context-aware trust frameworks can adapt to changes in user behavior, environmental conditions, or task requirements, allowing for more resilient and efficient trust evaluations.

Decentralized, incentive-compatible strategies also hold promise in addressing scalability and resilience. Blockchain-based trust models, such as the one introduced by Mssassi and Kalam, offer tamper-proof recording of trust events and enable distributed reputation management without centralized control [21]. However, current implementations face challenges related to latency and energy consumption. Future work should explore lightweight consensus protocols, micro-incentive schemes, and adaptive trust score propagation to balance the benefits of decentralization with practical efficiency. These strategies can enhance cooperation and deter malicious behavior by aligning individual incentives with collective network goals, even in fully decentralized or intermittently connected environments.

Cross-layer trust modeling presents another fertile research area. Rather than isolating trust assessment at the application layer, future models should consider trust signals from multiple network layers—such as physical signal integrity, transport-level packet loss, and application-level behavior. Such integration could provide a holistic view of trustworthiness and improve accuracy in identifying threats like jamming, spoofing, or selective forwarding. Farrahi and Zia's work on trust diffusion through friendship networks offers insight into the social dimension of trust, suggesting that trust cues can emerge from user behavior patterns across communication protocols [26]. A cross-layer approach could further uncover hidden vulnerabilities and strengthen defense mechanisms against complex, multi-layer attacks.

Lastly, privacy-aware trust computation is becoming increasingly vital. As networks grow in size and heterogeneity, the potential for data exposure and inference attacks also increases. Future trust models must incorporate privacy-preserving techniques, such as homomorphic encryption, differential privacy, or federated learning, to ensure that sensitive data used in trust calculations is protected. The model proposed by Horita and Yamazaki, which correlates generalized trust with social behaviors, underscores the importance of privacy in trust analysis, particularly in systems where trust evaluation involves sensitive personal or behavioral data [27]. Protecting user privacy while maintaining trust transparency is a delicate balance that future research must address through innovative cryptographic and architectural solutions.

In conclusion, the future of game theory-based trust modeling in infrastructure-free social networks lies in embracing hybridization, contextual intelligence, decentralization, and cross-disciplinary integration. By addressing existing challenges and exploring these promising directions, researchers can develop more resilient, adaptive, and deployable trust systems capable of operating under the complex realities of modern decentralized environments.

8. Conclusion

The growing reliance on infrastructure-free social networks, such as MANETs, VANETs, DTNs, and emerging IoT and UAV environments, has made trust management a cornerstone of secure and reliable communication. These networks operate in highly dynamic, decentralized, and often unpredictable settings, where traditional centralized security mechanisms are either ineffective or entirely inapplicable. In this context, trust modeling becomes essential—not just as a means of ensuring data integrity and network performance, but also as a mechanism for fostering cooperation, deterring malicious behavior, and adapting to changing circumstances in real time.

Game theory has emerged as a powerful and flexible framework for trust modeling in these settings. Its ability to capture the strategic behavior of rational agents, whether cooperative or competitive, makes it particularly well-suited for the complex decision-making processes inherent to decentralized networks. Through its various forms—including non-cooperative games, cooperative games, evolutionary games, and Bayesian or repeated game structures—game theory provides diverse modeling approaches that align with different network needs and constraints. Each approach offers distinct advantages and trade-offs. Non-cooperative games are straightforward and scalable, yet they often lack robustness against adversarial behavior. Cooperative models foster collaboration and fair resource sharing but come at the cost of increased overhead. Evolutionary games allow adaptation and learning but may require time to stabilize, while Bayesian and repeated games offer nuanced decision-making under uncertainty, often at the expense of computational complexity.

Across the literature, a rich variety of game-theoretic trust models has been developed, each tailored to specific network types, threat scenarios, and operational goals. Some models prioritize rapid trust decisions for highly mobile environments, while others focus on long-term stability and resilience. The comparative analysis shows that while there is no one-size-fits-all solution, the strategic principles of game theory offer a solid foundation for the development of adaptive, responsive, and context-aware trust mechanisms. However, several limitations and challenges remain. These include issues of scalability, particularly in dense or resource-constrained networks; the vulnerability of trust models to collusion or strategic deception; the difficulty of maintaining reliable trust assessments in highly dynamic topologies; and the underexplored potential of integrating artificial intelligence and machine learning into game-theoretic frameworks.

Another critical gap lies in the lack of empirical validation. Many existing models are grounded in simulations or theoretical constructs, with limited application in real-world scenarios. As infrastructure-free networks become increasingly embedded in critical systems such as autonomous transportation, emergency response, and smart infrastructure, the need for validated, scalable, and robust trust models becomes even more pressing. Trust modeling cannot remain a purely theoretical pursuit—it must evolve into a practical, implementable framework capable of operating under real-world conditions with real-time constraints and diverse user behaviors.

Looking forward, the future of game theory-based trust modeling will likely be shaped by interdisciplinary integration. Combining game theory with data-driven methods such as machine learning can enable predictive trust evaluation and rapid anomaly detection. Incorporating cross-layer insights and context-awareness can enhance the precision and reliability of trust metrics. Decentralized and privacy-preserving mechanisms, such as blockchain and federated learning, can improve transparency while protecting sensitive data. These directions not only promise technical improvements but also align trust modeling with emerging expectations for fairness, accountability, and resilience in digital systems.

In conclusion, game theory continues to offer a compelling framework for trust modeling in infrastructure-free social networks. Its theoretical versatility and strategic depth have led to significant advancements in understanding and managing trust under conditions of uncertainty, decentralization, and conflict. However, its full potential remains to be realized. By addressing current limitations and embracing future research directions, the next generation of trust models can become not only smarter and more secure but also truly transformative in their ability to support complex, distributed communication systems in a rapidly evolving digital world.

Authors’ Contributions

Authors equally contributed to this article.

Acknowledgments

None.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethical Considerations

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

References

[1] Y. S. Razin and K. M. Feigh, "Committing to Interdependence: Implications From Game Theory for Human-Robot Trust," 2021, doi: 10.48550/arxiv.2111.06939.

[2] Y. Li, W. Fang, W. Zhang, W. Gao, and B. Li, "Game-Based Trust in Complex Networks: Past, Present, and Future," *Complexity,* vol. 2021, no. 1, 2021, doi: 10.1155/2021/6614941.

[3] M. S. Abdalzaher, K. G. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. B. Abdel-Rahman, "Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey," *Sensors,* vol. 16, no. 7, p. 1003, 2016, doi: 10.3390/s16071003.

[4] S. Bai, T. Zou, and X. Rong, "Research on Energy Efficiency Application of Wireless Communication Energy Saving and Emission Reduction Based on Self-Organizing Network Game Technology," *Journal of Physics Conference Series,* vol. 1802, no. 2, p. 022019, 2021, doi: 10.1088/1742-6596/1802/2/022019.

[5] M. Kejriwal, "Simulating and Quantifying Inequality in Strategic Agent Networks," 2023, doi: 10.54941/ahfe1004025.

[6] U. Grandi, E. Lorini, A. Novaro, and L. Perrussel, "Strategic Disclosure of Opinions on a Social Network," 2016, doi: 10.48550/arxiv.1602.02710.

[7] Y. Dong, J. Liu, J. Ren, Z. Li, and W. Li, "Modelling Attack and Defense Games in Infrastructure Networks With Interval-Valued Intuitionistic Fuzzy Set Payoffs," *Complex & Intelligent Systems,* vol. 10, no. 5, pp. 6249-6265, 2024, doi: 10.1007/s40747-024-01495-z.

[8] A. Y. Al-Zahrani and N. Thomas, "Analysing the Performance of a Trust-Based AODV in the Presence of a Flooding Attack," *Applied Sciences,* vol. 14, no. 7, p. 2874, 2024, doi: 10.3390/app14072874.

[9] W. Raub, V. Frey, and V. Buskens, "Strategic Network Formation, Games on Networks, and Trust," *Analyse & Kritik,* vol. 36, no. 1, pp. 135-152, 2014, doi: 10.1515/auk-2014-0106.

[10] Y. Wang, Z. Cai, G. Yin, Y. Gao, and Q. Pan, "A Trust Measurement in Social Networks Based on Game Theory," pp. 236-247, 2015, doi: 10.1007/978-3-319-21786-4_21.

[11] X. Li and S. Li, "A Trust Valuation Model Based on Game Theory in Social Network," 2016, doi: 10.2991/mmebc-16.2016.248.

[12] S. H. Chen, B.-T. Chie, and T. Zhang, "Network-Based Trust Games: An Agent-Based Model," *Journal of Artificial Societies and Social Simulation,* vol. 18, no. 3, 2015, doi: 10.18564/jasss.2767.

[13] U. Ravale, A. Patil, and G. M. Borkar, "Trust Management: A Cooperative Approach Using Game Theory," 2023, doi: 10.5772/intechopen.102982.

[14] S. Dhakal, R. Chiong, M. Chica, and T. A. Han, "Evolution of Cooperation and Trust in an N-Player Social Dilemma Game With Tags for Migration Decisions," *Royal Society Open Science,* vol. 9, no. 5, 2022, doi: 10.1098/rsos.212000.

[15] F. Zhang, J. Cao, Z. Wu, and Q. Wei, "Evolutionary Game Analysis of Construction Worker Safety Supervision Based on Complex Network," *Buildings,* vol. 15, no. 6, p. 907, 2025, doi: 10.3390/buildings15060907.

[16] M. Nojoumian, "Rational Trust Modeling," pp. 418-431, 2018, doi: 10.1007/978-3-030-01554-1_24.

[17] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and Q. Han, "A Game Theory-Based Trust Measurement Model for Social Networks," *Computational Social Networks,* vol. 3, no. 1, 2016, doi: 10.1186/s40649-016-0027-x.

[18] M. Tolkachov *et al.*, "Development of a Method for Protecting Information Resources in a Corporate Network by Segmenting Traffic," *Eastern-European Journal of Enterprise Technologies,* vol. 5, no. 9 (131), pp. 63-78, 2024, doi: 10.15587/1729-4061.2024.313158.

[19] J. Li, W.-H. Wu, Z.-Z. Li, W.-X. Wang, and B. Zhang, "Data-Driven Evolutionary Game Models for the Spread of Fairness and Cooperation in Heterogeneous Networks," *Frontiers in Psychiatry,* vol. 14, 2023, doi: 10.3389/fpsyt.2023.1131769.

[20] Y. S. Razin and K. M. Feigh, "Committing to Interdependence: Implications From Game Theory for Human–robot Trust," *Paladyn Journal of Behavioral Robotics,* vol. 12, no. 1, pp. 481-502, 2021, doi: 10.1515/pjbr-2021-0031.

[21] S. Mssassi and A. A. E. Kalam, "Game Theory-Based Incentive Design for Mitigating Malicious Behavior in Blockchain Networks," *Journal of Sensor and Actuator Networks,* vol. 13, no. 1, p. 7, 2024, doi: 10.3390/jsan13010007.

[22] Y. Chen *et al.*, "The Connectome-based Prediction of Trust Propensity in Older Adults: A Resting-state Functional Magnetic Resonance Imaging Study," *Human Brain Mapping,* vol. 44, no. 11, pp. 4337-4351, 2023, doi: 10.1002/hbm.26385.

[23] Y. Wang, X. He, J. Zuo, and R. Rameezdeen, "Ability or Morality? Exploring the Multiple Dimensions of Social Trust on Public Acceptance of Urban Transport Infrastructure Projects," *International Journal of Managing Projects in Business,* vol. 16, no. 2, pp. 301-324, 2023, doi: 10.1108/ijmpb-07-2022-0152.

[24] R. Thanappan and T. Perumal, "Congestion Aware MANET Routing Using Evolutionary Game Theory and Cross-Layer Design," *Ecs Transactions,* vol. 107, no. 1, pp. 1699-1709, 2022, doi: 10.1149/10701.1699ecst.

[25] Z. Erturkoglu, J. Zhang, and E. Mao, "Pressing the Play Button," *International Journal of E-Business Research,* vol. 11, no. 3, pp. 54-71, 2015, doi: 10.4018/ijebr.2015070104.

[26] K. Farrahi and K. Zia, "Trust Reality-Mining: Evidencing the Role of Friendship for Trust Diffusion," *Human-Centric Computing and Information Sciences,* vol. 7, no. 1, 2017, doi: 10.1186/s13673-016-0085-y.

[27] Y. Horita and M. Yamazaki, "Generalized Trust Rather Than Perception of Relational Mobility Correlates With Nominating Close Friends in a Social Network<sup>1</Sup>," *Japanese Psychological Research,* 2023, doi: 10.1111/jpr.12451.