UDC 004.891.3
IRSTI 50.41.25

https://doi.org/10.55452/1998-6688-2025-22-2-37-53

[1]*Moldabayev D.A.,
Master's student, ORCID ID: 0000-0001-8389-2953,
*e-mail: d_moldabayev@kbtu.kz
[1]Tinal M.B.,
Master's student, ORCID ID: 0000-0002-5503-0077,
e-mail: m_tinal@kbtu.kz
[1]Kartbayev A.Zh.
PhD, ORCID ID: 0000-0003-0592-5865,
e-mail: a.kartbayev@gmail.com

[1]Kazakh-British Technical University, Almaty, Kazakhstan

DEVELOPMENT OF A PRACTICAL APPROACH FOR INFORMATION CONFRONTATION MODELING IN SOCIAL NETWORKS BASED ON GAME THEORY METHODS

Abstract

This study investigates the dynamics of social networks in the context of information confrontation between users. It introduces a simulation method for modeling these conflicts, which is based on game-theoretic and probabilistic approaches. The paper suggests a method for dynamically observing, following, and updating the status of the network. This innovative method conceptualizes information conflicts as a two-player game where the objective is to control as many network nodes as possible. By applying game theory, we formulated a strategy adaptation algorithm that allows each player to modify their decision-making based on the Facebook Researcher open dataset and current network conditions of its Kazakhstani segment. The method for tracking the network's state dynamically leads to significant reductions in resource use and enhancements in computational efficiency. Comparative computational tests against other methodologies demonstrate the practical value of our approach for addressing a broad spectrum of challenges in information and analytical systems.

Keywords: game theory, strategy adaptation, Social networks, information conflict, simulation algorithm, probabilistic approach, analytical systems.

Introduction

This study addresses the critical challenge of analyzing social networks, which have become central to information dissemination, communication, and entertainment in contemporary society. The increasing prevalence and intricacy of social networks underscore the urgency of developing sophisticated analytical methodologies. Current data indicate that an average individual dedicates approximately 144 minutes daily to social media, a figure that has seen a consistent rise over the past decade. This trend underscores the significance of social networks as venues for information conflicts, including manipulation efforts and the dissemination of false information.

Generally, the issue of modeling the influence and management of information on social networks has been explored since the late 1990s [1]. The lack of stringent regulatory oversight and the anonymity afforded by the internet present opportunities for malicious entities to propagate harmful content. Information warfare, encompassing a spectrum of scenarios where information is weaponized to achieve specific objectives, often involves conflicting interests among different parties. Examples include corporate rivalries, political disputes, propaganda campaigns, and efforts to counteract misinformation and manipulation. Given these considerations, investigating the structure of social networks to bolster online security, prevent the spread of harmful content, and combat issues like botnets is of paramount importance. The evolving complexity and dynamism of social networks challenge existing analytical methods, necessitating the development of new, more effective, and efficient solutions [2].

This research introduces an innovative approach to social network analysis within the framework of information conflicts. It integrates game-theoretical principles with probabilistic models of information dissemination and dynamic network modeling. Additionally, it presents a sophisticated algorithm for real-time monitoring and strategy adjustment among network entities. The objective is to establish a model for information confrontation between two entities, designated as A and B, that surpasses existing methodologies in terms of efficiency and resource utilization. The validity and applicability of the proposed model are affirmed through extensive testing on large-scale network models, highlighting its relevance and practical utility in contemporary social network analysis.

The field of social network analysis includes a large number of research interests and methodologies, reflecting its significance in understanding complex social structures and behaviors. Studies in this domain have traditionally focused on varied aspects such as information warfare, community detection, node influence and centrality, viral information dissemination, recommendation systems, and sentiment analysis within networks. Various analytical techniques such as graph theory, machine learning, clustering, genetic algorithms, and game theory have been employed to dissect these phenomena [3].

Our research situates itself within the context of information confrontation in social networks, a key aspect of information warfare. The process of information dissemination forms a crucial component of this confrontation. Traditionally, models for information dissemination in social networks are categorized into graph-based and non-graph-based approaches. Among the graph-based models, the Independent Cascades (IC) model [4] and the Linear Threshold (LT) model [5] are particularly prominent.

The Linear Threshold model operates under the premise that a node becomes activated when the influence from its activated neighbors surpasses a predefined threshold. This model aptly simulates situations where community or group decisions are critical, effectively mirroring real-life scenarios like the adoption of new products or ideas once they gain sufficient traction within a community. This model also sheds light on social influences impacting decision-making, often cited in studies of phenomena such as the “tipping point effect.”

However, the LT model’s primary limitation is its focus on collective thresholds rather than individual decision-making processes, which are vital in networks where personal decisions are pivotal. While both models operate on a discrete time axis where the information dissemination process is iterative and synchronous, starting from initially activated nodes [6], there have been adaptations to enhance their applicability and efficiency. For instance, some studies have introduced variations of the LT model that incorporate factors like content virality and user-specific probabilities of information acceptance [7]. Additionally, asynchronous versions of these models have been developed to optimize resource usage and improve computational efficiency, addressing some of the synchronous models’ limitations [8].

In addition to graph-based approaches, models that do not rely explicitly on predefined network structures, such as the Susceptible-Infectious-Recovered (SIR) and Susceptible-Infectious-Susceptible (SIS) models, are instrumental in understanding network dynamics [9]. These epidemiological models assess the state of each node and track changes in population segments over time using differential equations. They operate under the assumption of random interactions among nodes, which simplifies the analysis but might not capture the unique structural properties of specific social networks, thus limiting their detailed applicability to social phenomena.

Further enriching the toolkit for social network analysis, probabilistic models, influence maximization algorithms like Cost-Effective Lazy Forward (CELF) and CELF++, network monitoring optimization algorithms, and game-theoretic frameworks for modeling information influence have also been developed [9, 10, 11]. Game-theoretic approaches, in particular, have gained prominence. For example, one study employs game theory to devise strategies for blocking influence maximization using oracles to generate mixed strategies for the players, while another builds on this with a hierarchical algorithm to enhance the method's efficiency [12, 13].

The limitations of existing approaches often revolve around the assumption of static network conditions–despite the inherently dynamic nature of real networks–or the substantial computational resources required for processing complex network structures. The ongoing escalation in network complexity further complicates the analysis of modern networks using traditional methodologies. To address these challenges, we introduce a novel game-theoretic model combined with Markov probabilistic models for information dissemination.

This hybrid model incorporates a streamlined one-oracle approach to reduce computational demands while capturing the dynamic interactions and strategic behaviors of entities within the network. The specifics of this model and its application are explored in subsequent sections of this study, where we detail its design, implementation, and the insights it offers into effective information warfare strategies between players A and B.

Any social network can be depicted as a graph G = (V, E), where V represents the vertices, corresponding to user accounts, and E denotes the edges, signifying the connections between these accounts. These graphs may be either directed or undirected. In a directed graph, connections have a specific orientation, meaning that if user A follows user B, it does not necessarily imply that user B follows user A. Twitter is a typical example of a directed graph, while networks like Facebook are examples of undirected graphs.

The process of information dissemination on social media can cause certain pieces of information to gain fame and even become viral, spreading rapidly across the globe. This process generally unfolds in two primary stages:

- Initial Distribution: Information is shared within a user's immediate circle through personal messages or public posts.
- Further Distribution: The information then propagates along the network's edges according to the specific rules of the graph that models the network.

Each user within a social network exercises their judgment to either trust or dismiss the information they encounter. Furthermore, the decision of each user is influenced by the opinions and actions of others within the same network, a phenomenon known as social influence [13]. One straightforward method to model the dissemination of information is to consider each node in the graph as activated if the node receives and accepts the information, and not activated if the node either does not receive or does not accept it.

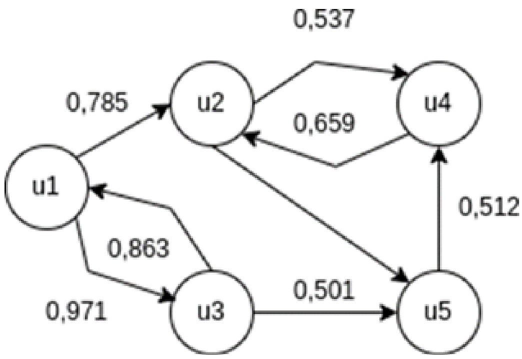

Figure 1 – A directed graph with 5 users and connections between them

Figure 1 illustrates a directed graph connecting five users. In this diagram, the weights on each edge indicate the strength of the connection between users. A higher weight suggests a greater level of trust between the users, which is crucial in the context of information dissemination, as users with stronger or more influential connections are more likely to trust each other. This modeling approach is visualized in Figure 2, where nodes that have accepted the information are highlighted in red. Then we adopt this modeling strategy in our research.

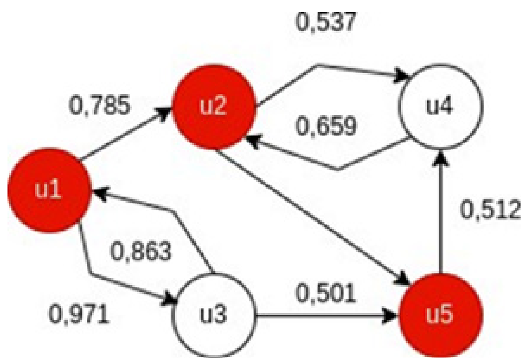

Figure 2 – The process of node activation during the information diffusion

Materials and Methods

The Information Influence Model is designed to explore the impact of information on user behavior. Its primary objective is to determine how the information environment and the user's awareness of information shape their decision-making processes. By employing this model, researchers can analyze how information flows within a network affect user behavior and decision-making. Because social networks can be used as the arena for various types of information confrontation, when analyzing social networks in the context of this confrontation, traditionally, three main nested classes are analyzed: Information Influence, Information Management, and Information Confrontation, as shown in Figure 3.

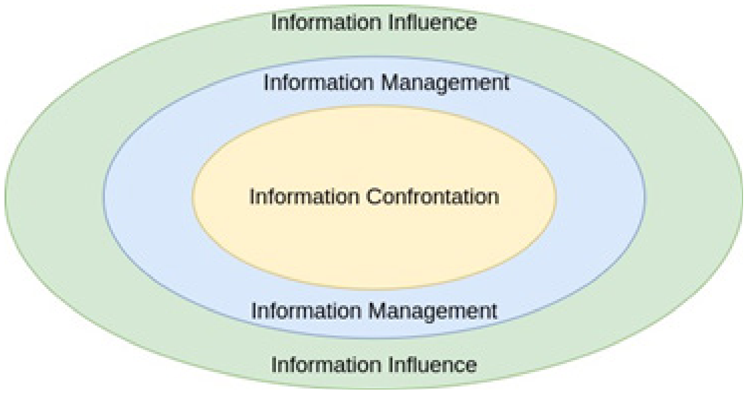

Figure 3 – A model of information influence, management and confrontation

Expanding upon the Information Influence Model, the Information Management Model introduces an additional layer of complexity by incorporating deliberate control over user behavior through targeted information influence. This extension allows for a more nuanced understanding of how information can be strategically managed to guide or alter user behaviors within the network [14]. This approach is crucial for studies aimed at understanding the dynamics of information control and its implications on individual and collective actions within social networks.

The main task of this model is to develop strategies to affect the user in a desired way. For instance, given two players A and B each of which can influence the initial opinions of certain agents in the network. Let $A \subseteq N$ be the set of agents, whose opinions are formed by player A, and $B \subseteq N$ be the set of agents whose opinions are formed by player B, then $A \cap B = \emptyset$.

Let us assume that information management is unified [15], meaning that all agents in the set A form initial opinions $u \in U$, and all agents in the set B form initial opinions $v \in V$, where U and

$V \subseteq R$. The change in the opinion of a network agent, taking into account his own opinion, as well as the opinions of his surrounding neighbors, can be represented as an expression (1):

$$xti = \sum aij * xjt\text{-}1,\ t = 1,2, \dots,\ i \in N. \quad (1)$$

According to [16] this expression (1) can be simplified as $X = \sum rj*xj0$ and in the context of information management can be expanded to $X(u,v) = rAu + rBv + X0$, meaning that the final opinion of the social network agents is linearly dependent on management factors u and v with the weights $rA > 0$ and $rB > 0$, where $rA + rB <= 1$.

Finally, using the model of information management makes it possible to model the information confrontation between users having opposing interests and wanting to influence the subjects of the network. To form a game-theoretic model of player interaction, it is necessary to determine the objective function of each player. For instance, the objective function of a certain player can be determined as follows [17]:

$$f(u,v) = QA(X(u,v)) - CA(u), \quad (2)$$

where QA(X(u,v)) is the quality function of changing the opinion of a particular agent by player A; CA(u) is the cost function, i.e. the resources spent by player A to change the opinion of a certain agent.

Consequently, [15] states that the population of objective functions $G = \{fA(u,v), fB(u,v), u \in U, v \in V\}$ and sets of possible actions result in family of games, the differences between which are generated by the specification of the players' information and the order of functioning. If the description of the game and the expression of changing the agent's opinion are common among all players who make their choices only once, simultaneously and independently, then we obtain a game in normal form. In such a game it is possible to search for the Nash Equilibria and assess the effectiveness of player moves by Pareto. According to game theory, the Nash equilibria is a situation in a non-cooperative game where each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only their own strategy unilaterally. Mathematically it is expressed as follows:

$$Ui(si^*, s\text{-}i^*) >= U(si, s\text{-}i^*), \quad (3)$$

where U_i is the payoff function for player i; s_i* is the strategy chosen by player i in the Nash equilibrium; s_{-i}* is the strategies chosen by all other players in the Nash equilibrium.

According to [18], two primary principles govern social influence within a social network: herd behavior and information cascades. An information cascade occurs when users disregard their own opinions and adopt the views or behaviors of others, based on the assumption that these others have acted on valid information–even if such information may not actually be sound. This process leads individuals to follow a chain reaction of decisions made by predecessors without critically evaluating the underlying information [19].

On the other hand, herd behavior involves individuals mimicking the decisions and actions of others but with the flexibility to modify these actions based on their personal perspectives. In this scenario, while individuals are influenced by the group, they do not completely abandon their own judgments or insights. In our research, we have developed a model that incorporates these concepts of social influence. This model is visually represented in Figure 4. Let us now delve deeper into each component of the depicted scheme to understand how these dynamics of social influence are integrated and modeled.

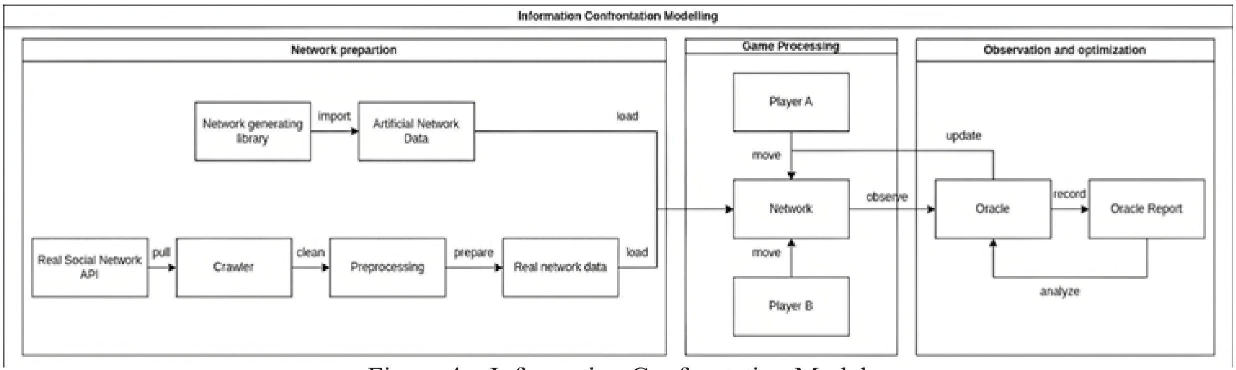

Figure 4 – Information Confrontation Model

First of all, we designed an artificial network (See Figure 5) using the Networkx, a Python library, to model different experiments and compare the results. We apply standard graph theory methods to model the social network. We have graph G = (V, E) where vertices (V) are social network accounts and edges (E) are connections between them. Each vertex in the graph has a list of parameters required to process the model. As it is an information confrontation model, each node of the graph has the following parameters:

`A_trust_prob`, i.e. 0.1 <= `A_trust_prob` <= 1: shows the probability that a user will be activated by player A;

`A_trusted`, i.e. `A_trusted` ∈ {1, 0}: shows whether or not a user has been activated by player A;

`B_trust_prob`, i.e. 0.1 <= `B_trust_prob` <= 1: shows the probability that a user will be activated by player B;

`B_trusted`, i.e. `B_trusted` ∈ {1, 0}: shows whether or not a user has been activated by player B;

`spread_factor`, i.e. 0 <= `spread_factor` <= 1: shows the ability of the user to spread gained information further to its neighbors;

`activity_rate`, i.e. 0 <= `activity_rate` <= 1: shows how active the user is in the network.

To show the strength of connections between users, we integrated the weight factor upon each edge, showing the trust level (`trust_level`, i.e. 0 <= `trust_level` <= 1) between the users. With the help of this simulated network, we have conducted plenty of experiments, which will be discussed in detail in the “Results” section.

However, having just an artificial network is not enough to make solid conclusions, so we decided to test our algorithm on real social networks. For that purpose, we decided to program the crawler system, which will be integrated with real social network APIs and pull publicly available data required for information confrontation modeling [20].

Then, the data will be cleaned and preprocessed, and after that, based on this data, the network model will be created and injected into the confrontation game. To keep the network dynamic, the Crawler will periodically pull new data from the actual network and inject it into our game. The part of the research that includes real-world network integration is currently in progress. That is why all the experiments presented in this paper are performed on the designed artificial network.

Game Processing. We modeled information confrontation as the game of two players, A and B, that fight for influence in a particular social network. It can be two companies that want to gain the trust and loyalty of users. Each player aims to spread its information across as many users in social networks as possible, having limited resources. To reach this goal effectively, a player should adapt his strategy to respond to the changing environment, considering the current network state and the predicted opponent’s strategy. A player has three options to move:

- It can send information to a particular user (i.e., try to activate it)
- It can try to switch the user activated by its opponent, thus luring the user to its side
- It can try to increase the likelihood that a particular user will believe his information

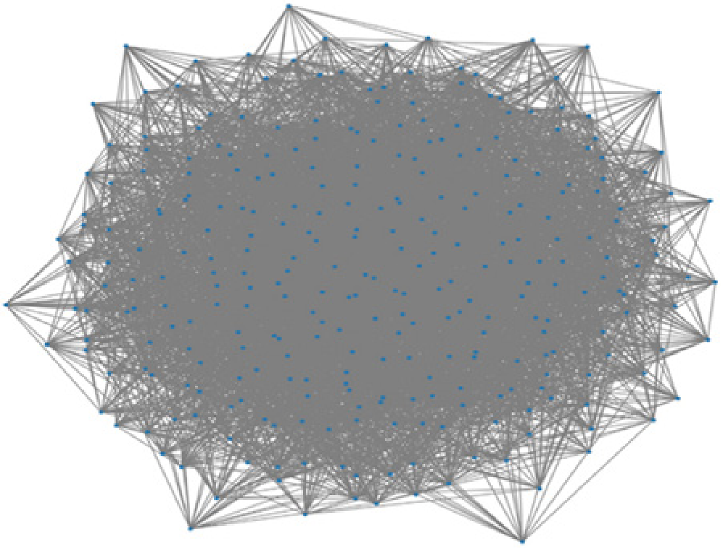

Figure 5 – Artificial network model with 300 nodes

If the node is activated by player A it is colored red and if it is taken by player B it is colored blue. All other nodes are represented as gray. Figure 6 shows how the information diffusion is generated by two players in our network model. The game lasts for a number of rounds settled at the initialization phase. At each round of the game, players choose the best move according to the cost function, i.e., the move that brings the highest profit to the user is selected. In our game, this cost function is as follows:

$$Q = P(activation)_{curr} * S_{factor_{curr}} * A_{rate\ curr} + \sum i \in Neighbors(trust\_level(curr, i) * P(activation)_i * S\_factor_i * A\_rate_i)'$$

where P(activation)curr – the probability that the current node will be activated by the given player; S_factorcurr – the ability of the current node to spread information further; A_ratecurr – the activity level of the current node in the network; trust_level(curr, i) – trust level between current node and its neighbor I; P(activation)i – the probability that the neighbor i of the current node will be activated by the given player; S_factori – the ability of the neighbor to spread information.

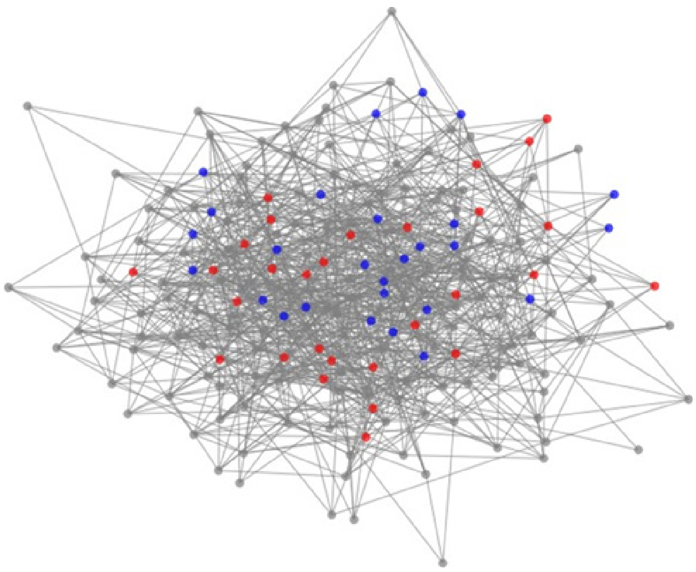

Figure 6 – Information diffusion process generated by two players

This quality function considers not only the current node's parameters but also its neighbors' parameters to identify the nodes, the activation of which will maximize the spread of the information of the given player. This function also considers the willingness of the user to spread information further at a given time. For instance, the user may have a high spread factor, but at a given time, it may not want to spread information for some reasons such as bad mood, fatigue, frustration, etc [21]. It is accomplished by including the randomness factor in the model to make nodes act like real-world social network users.

Real-world social network users depend on plenty of random factors such as mood, fatigue level, engagement in social network activity, etc. Therefore, it is essential to consider such factors when modeling the information dissemination process. The algorithm of how each player selects its best move at a given time is shown in Figure 7.

Listing 1.0. Player's best move algorithm

Inputs:
R - current player's resources,
$G_{not\_activated}$ - the subset containing not activated nodes of the current player

Output:
player's best move

1. Begin
2. Iterate through the set of inactivated nodes of the current player:
   a. Apply the cost function to each node
   b. Find the node with the highest quality
3. If the selected node is not activated by the opponent:
   a. If it is possible to activate it right now:
      i. Activate this node
      ii. Remove this node from the current player's set of inactivated nodes
      iii. Reduce the resources of the current player
   b. Else if it is not possible to activate it right now:
      i. Increase its activation probability by 0.1
      ii. Reduce the resources of the current player
4. If the selected node is activated by the opponent:
   a. If it is possible to switch the node right now:
      i. Switch it
      ii. Remove this node from the current player's set of inactivated nodes
      iii. Add this node to the opponent's set of inactivated nodes
      iv. Reduce the resources of the current player
   b. Else if it is not possible to switch it right now:
      i. Increase its activation probability by 0.1
      ii. Reduce the resources of the current player
5. End

Figure 7 – The algorithm of player selection

Observation and Optimization. To optimize the model's performance, we designed an Oracle that constantly monitors the network and its state [22]. This oracle tracks all the changes in the network at a given time and documents them in the report. With the help of this oracle, we can visualize the network and the state of each element at any given time during the model's execution. This oracle also keeps track of the inertial network changes provoked by a specific node's activation.

These so-called "inertia changes" occur when an activated node tries to activate its neighbors without the engagement of any player. Using such an oracle significantly increases the speed of computations and minimizes the amount of resources consumed by the game. The process of network state tracking and actualization is represented in Figure 8.

Listing 2.0. Network actualization and inertial effect after each move

Input:
G - social network graph

Output:
Actualized network

1. Begin
2. If the last move was 'activate' or `switch`:
    a. Update Oracle's report
    b. If the node is able to spread information to its neighbors and is willing to do that:
        i. Take a random subset of neighbors this node is willing to share information with
        ii. Run through each neighbor in this subset and try to activate it:
            1. If neighbor is not activated by the opponent:
                a. If neighbor can be activated:
                    i. Activate it
                    ii. Remove it from the current player's set of inactivated nodes
                b. Else:
                    i. Skip this neighbor
            2. Else if neighbor is activated by the opponent:
                a. If neighbor can be switched by the current player:
                    i. Switch it
                    ii. Remove it from the current player's set of inactivated nodes
                    iii. Add it to the opponent's set of inactivated nodes
                b. Else:
                    i. Skip this neighbor
    c. Else:
        i. Do nothing
3. Else if the last move was `increase trust_prob`:
    a. Update Oracle's report
4. End

Figure 8 – The algorithm of network state tracking

The Independent Cascade model describes a scenario where each activated node has a single opportunity to activate each of its inactivated neighbors with a specific probability. This model is particularly suited to scenarios that mimic the viral spread of information, where one node's activation can lead to a chain reaction across the network. Nevertheless, the IC model's simplicity—each node having only one chance to activate its neighbors—may not fully capture the repeated efforts users often make in real interactions, nor does it accommodate the long-term dynamics of node interactions within continually evolving networks.

Results

In this research, we proposed a novel approach for modeling information warfare between users in social networks based on game theory methods, probabilistic approaches for describing the spread of information, and dynamic algorithms for monitoring and tracking the state of the network at a given time. To find out how well the model does its job, we conducted several experiments on our artificial network, and we plan to conduct experiments on a real-world network in the future.

First of all, we ran the model and analyzed how well two players adapted their strategies during the game. Several experiments conducted on networks with different numbers of nodes confirmed that users were able to effectively change their strategies according to the changing environment to gain maximum profit from each step. For instance, the results of a confrontation game with 100 rounds between two players A and B having limited resources in the network with 500 nodes, are shown in Figure 9.

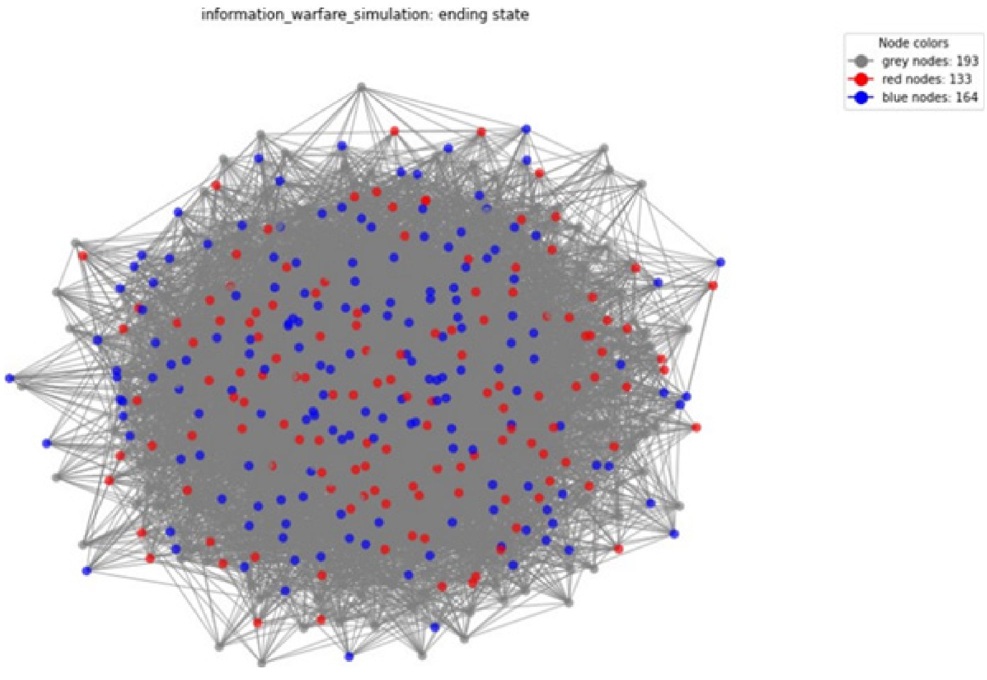

Figure 9 – Confrontation in the network with 500 nodes

Furthermore, we conducted comparison tests with other existing methods. The results of the experiments were compared with those of existing IC and LT models. We evaluated the efficiency of each approach based on its ability to maximize the spread of the information in the network, taking into account the initial limitations of resources. We compared the elapsed time of each approach and RAM and CPU usage on the networks with the different number of nodes. The performance comparison is represented in Figure 10. However, these methods face challenges when applied to large-scale real-world networks due to their computational intensity and time requirements. For instance, identifying optimal nodes for monitoring a Twitter subnetwork with 11,000 nodes and 25,000 connections required approximately 28.7 hours in one study, highlighting the significant resource demands of these analyses.

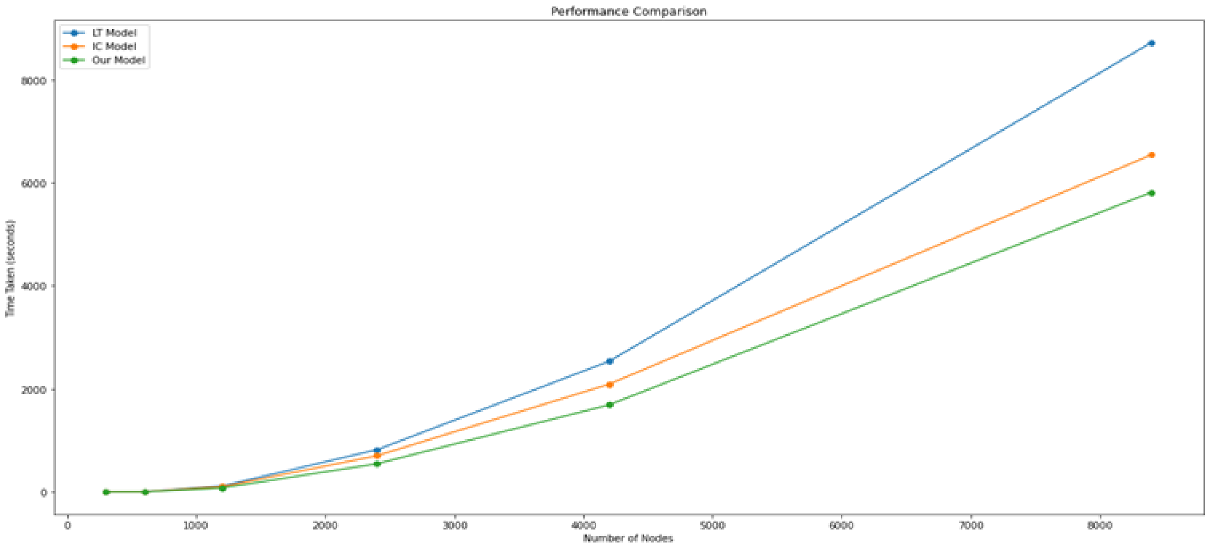

Figure 10 – Performance comparison of the approach

As can be seen from the graph, when the number of nodes was significantly small, all three models showed approximately similar results. However, when the number of nodes exceeded 1000, our model showed slightly better results than the others. Moreover, the execution time gap between these models became more prominent as the number of nodes in the network increased.

Since we progress to the second phase of this research, which involves integration with a real-world network, we plan to further evaluate and compare the performance and resource utilization of these models in an actual social network setting. This upcoming comparison will provide deeper insights into the efficiency and practicality of our model when applied to real-world data, potentially confirming its viability for broader use. The approach significantly increases the validity of the model since it becomes capable of verification based on current data, thereby ensuring a high level of reliability of research conclusions.

Comparative analysis of our approach with existing models, such as Linear Threshold and Independent Cascade models, revealed meaningful findings. While our model demonstrated competitive RAM and CPU utilization, especially on large networks, nuanced differences in computational efficiency highlight the potential of our approach. The LT model has shown a consistent and predictable level of CPU consumption, indicating its linear thresholding mechanism, as shown in Figure 10. In contrast, the IC model's CPU usage has exhibited a more volatile pattern, reflecting the stochastic nature of the cascading process.

Thus, at the end of the experiment, when the number of nodes was approximately 10,000, our model could process them in 5814 seconds, whereas 6541 seconds and 8722 seconds were required for processing by IC and LT models, respectively. In terms of CPU and RAM, our model has also shown promising results. As represented on Figure 11 the IC Model consumed the highest amount of memory among those models, and our model consumed the least memory compared to the other models.

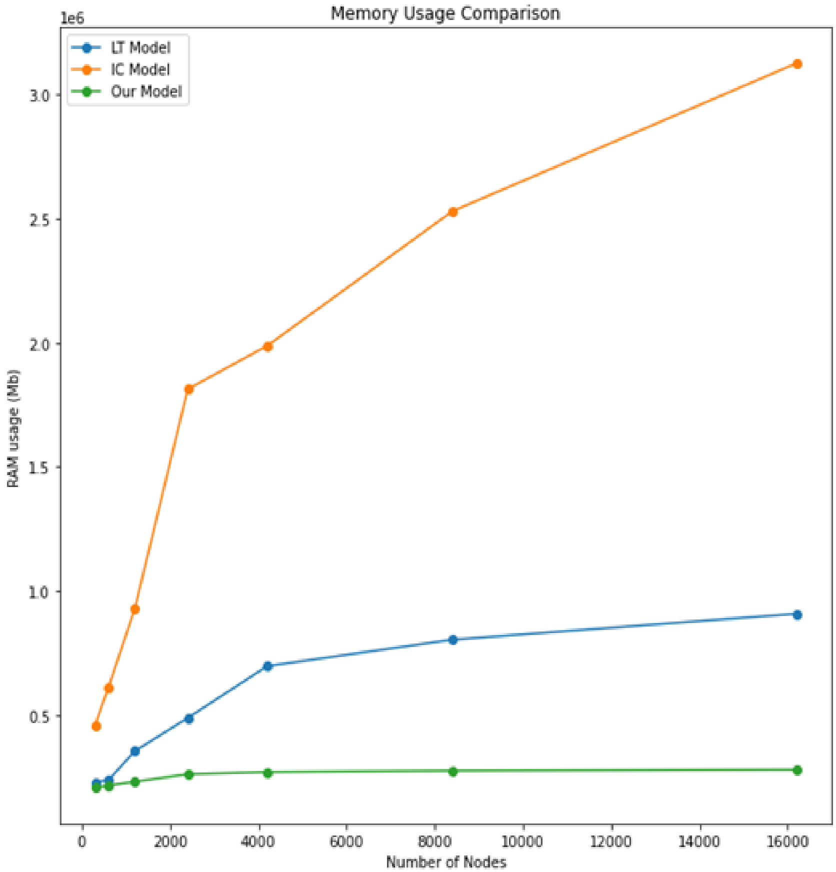

Figure 11 – Memory usage comparison with other models

The results suggest that the game theory approach maps well to the computational requirements of existing models and offers a robust framework for capturing the complex dynamics of information propagation. In particular, the zigzag pattern of CPU usage, as represented on Figure 12, in the IC model highlights the complex and unpredictable nature of the information cascade, which our game theory model handles more consistently and efficiently.

The model demonstrates superior performance in CPU consumption compared to the IC model, although it does not outperform the LT model. However, the difference in CPU usage between the LT model and our model is minimal and not significant. Overall, our model has delivered satisfactory outcomes across numerous tests conducted on an artificial network with varying numbers of nodes. Our algorithm can be used in many fields requiring social network modeling, including information confrontation modeling, network security, disinformation, viral content reduction, suppression of uprisings, and weakening of adverse effects on society.

Discussion

The advent of social networks has caused a paradigm shift in information dissemination, transforming the landscape of communication, influence, and decision-making processes. Therefore, understanding the dynamics of information confrontation in social networks is not just an academic interest but also an urgent need. Models designed to simulate these dynamics, especially using game theory methods, offer a perspective from which it is possible to decipher complex interactions and predict potential outcomes [23].

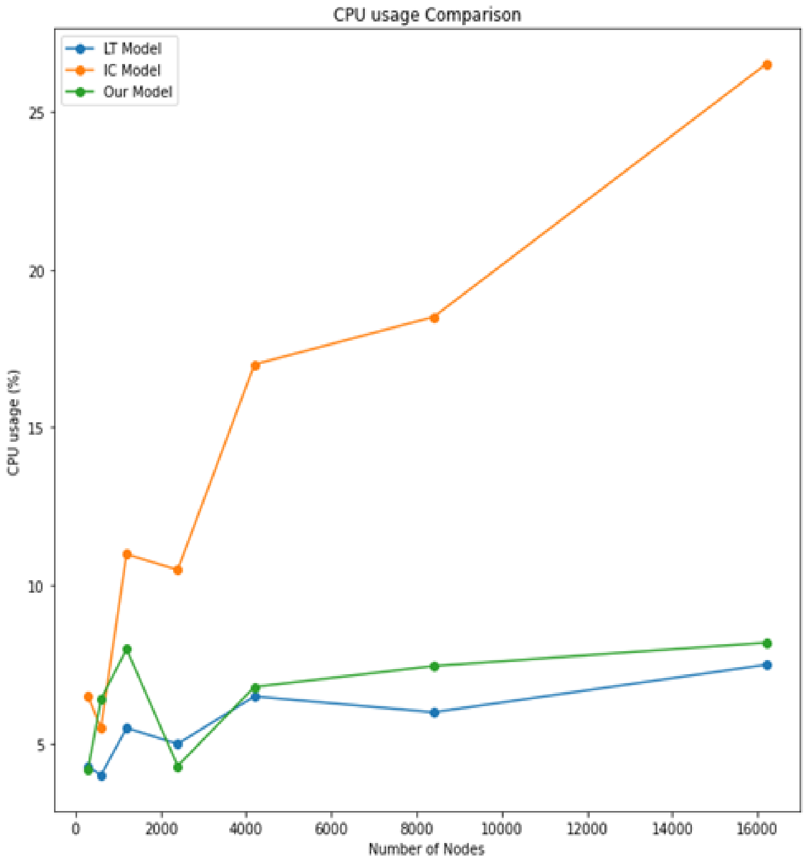

Figure 12 – CPU usage comparison with other models

The research began with the ambitious goal of modeling information confrontation in social networks using a new approach based on game theory. The pervasive nature of social networks and the multifaceted ways in which reliable and controversial information is disseminated on them emphasize the relevance of this study. As social networks become increasingly important in forming public opinions, political discourse, and market dynamics, the ability to analyze and predict the flow of information becomes crucial.

Conducted experiments allowed us to identify gaps in existing models, such as limited adaptability and predictability to dynamic changes in user behavior and network structure. Our approach provides deep insight into the interaction mechanisms in the information space, considering many factors, including probabilistic estimates and game theoretical strategies. The most notable novelty of our work is integrating game theory with dynamic probabilistic and monitoring algorithms, which allows real-time adaptation of information dissemination strategies. It represents a significant advance in information warfare research, offering a more granular and adaptive approach to managing information flows.

In future research, we plan to integrate an automatic crawler mechanism into our model that will be used to extract data through social network APIs, thereby ensuring that the input data for the modeling is up to date. This modification involves a significant deepening of the methodological approach by providing access to actual information flows and structures of social interactions. The resulting graph of a real social network will serve as the foundation for analytical work, allowing the model to operate with data reflecting the current state of social media.

Conclusion

In this research, we proposed a novel approach to analyze social networks in the context of information confrontation based on game theory, information dissemination probabilistic models, and network monitoring, tracking, and optimization dynamic algorithms based on one Oracle approach. Social networks are a vital part of modern people's lives, making social network analysis a relevant topic today.

The main advantage of our approach is that the whole process is dynamic, which makes it more realistic and natural. Using game theory allowed us to realistically model the process of information warfare and program adaptive strategies for each player. Our Oracle optimization algorithm helped us to overcome some limitations of existing methods by showing better results in elapsed time and resource consumption compared to other models.

In the upcoming research, we plan to integrate a real-world network into our model with the help of a crawler algorithm and data preparation and optimization tools. The part of the job is still in progress and will be revealed in the upcoming papers. This method has shown decent results and provides excellent prospects for developing the process of modeling and analyzing social networks.

REFERENCES

1 Wang J., Yang Y., Liu Q., Fang Z., Sun S., Xu Y. An empirical study of user engagement in influencer marketing on Weibo and WeChat // IEEE Transactions on Computational Social Systems. – 2023. – Vol. 10. – P. 3228–3240. https://doi.org/10.1109/TCSS.2022.3204177.

2 Sun B., Al-Bayaty R., Huang Q., Wu D.O. Game theoretical approach for non-overlapping community detection // Proceedings of the 5th International Conference on Big Data Computing and Communications. – 2019. – P. 222–230. https://doi.org/10.26599/TST.2020.9010017.

3 Bruning P.F., Alge B.J., Lin H.-C. Social networks and social media: Understanding and managing influence vulnerability in a connected society // Business Horizons. – 2020. – Vol. 63. – No. 6. – P. 749–761. https://doi.org/10.1016/j.bushor.2020.07.007.

4 Huang D., Tan X., Chen N., Fan Z. A memetic algorithm for solving the robust influence maximization problem on complex networks against structural failures // Sensors. – 2022. – Vol. 22. – No. 6. – P. 2191. https://doi.org/ 10.3390/s22062191.

5 Peng Y., Bai X. Identifying social tipping point through perceived peer effect // Environmental Innovation and Societal Transitions. – 2024. – Vol. 51. – P. 2367–2382. https://doi.org/10.1016/j.eist.2024.100847.

6 Liu Y., Bao Z., Zhang Z., Tang D., Xiong F. Information cascades prediction with attention neural network // Human-centric Computing and Information Sciences. – 2020. – Vol. 10. https://doi.org/10.1186/s13673-020-00218-w.

7 Rangnani S., Devi V.S. Predicting potential retweeters for a microblog on Twitter // Intelligent and Evolutionary Systems. – 2016. – Vol. 5. – P. 1–5. https://doi.org/10.1007/978-3-319-27000-5_14.

8 Qiang Z., Pasiliao E., Zheng Q. Model-based learning of information diffusion in social media networks // Applied Network Science. – 2019. – Vol. 4. – No. 1. – P. 1–16. https://doi.org/10.1007/s41109-019-0215-3.

9 Zhang L., Li K., Liu J. An information diffusion model based on explosion shock wave theory on online social networks // Applied Sciences. – 2021. – Vol. 11. – P. 9996. https://doi.org/10.3390/app11219996.

10 Bourigault S., Lagnier C., Lamprier S., Denoyer L., Gallinari P. Learning social network embeddings for predicting information diffusion // Proceedings of the 7th ACM International Conference on Web Search and Data Mining (WSDM '14). – 2014. – P. 393–402. https://doi.org/10.1145/2556195.2556216.

11 Newman M.E.J. The structure and function of complex networks // SIAM Review. – 2003. – Vol. 45. – P. 167–256. https://doi.org/10.1137/S003614450342480.

12 Tsai J., Nguyen T., Tambe M. Security games for controlling contagion // Proceedings of the AAAI Conference on Artificial Intelligence. – 2021. – Vol. 26. – No. 1. – P. 1464–1470. https://doi.org/10.1609/aaai.v26i1.8249.

13 Li Q., Du H., Li X.-Y. Influence of influence on social networks: Information propagation causes dynamic networks // Proceedings of the 2021 7th International Conference on Big Data Computing and Communications (BigCom). – 2021. – P. 278–285. https://doi.org/10.1109/BigCom53800.2021.00016.

14 Podlipskaia O. Determining effective strategies for information warfare in consolidated and polarized populations // Proceedings of the IEEE Conference on Machine Learning and Systems. – 2022. – P. 1–5. https://doi.org/10.1109/MLSD55143.2022.9934658.

15 Li T., Zhao Y., Zhu Q. The role of information structures in game-theoretic MAL // Annual Reviews in Control. – 2022. – Vol. 53. – P. 296–314. https://doi.org/10.1016/j.arcontrol.2022.03.003.

16 Ganai A.H., Hashmy R., Khanday H.A. Finding information diffusion's seed nodes in online social networks using a special degree centrality // SN Computer Science. – 2024. – Vol. 5. – P. 333. https://doi.org/10.1007/s42979-024-02683-x.

17 Genschow O., Klomfar S., d'Haene I., Brass M. Mimicking and anticipating others' actions is linked to social information processing // PLoS One. – 2018. – Vol. 13. – No. 3. – e0193743. https://doi.org/10.1371/journal.pone.0193743.

18 Papadopoulou O., Makedas T., Apostolidis L., Poldi F., Papadopoulos S., Kompatsiaris I. MeVer NetworkX: Network analysis and visualization for tracing disinformation // Future Internet. – 2022. – Vol. 14. – No. 5. – P. 147. https://doi.org/10.3390/fi14050147.

19 Iqbal S., Arif T., Malik M., Sheikh A. Browser simulation-based crawler for online social network profile extraction // International Journal of Web Based Communities. – 2020. – Vol. 16. – P. 321–342. https://doi.org/10.1504/IJWBC.2020.111377.

20 O'Neil D., Petty M. Heuristic methods for synthesizing realistic social networks based on personality compatibility // Applied Network Science. – 2019. – Vol. 4. – P. 141–158. https://doi.org/10.1007/s41109-019-0117-4.

21 Luo T., Cao Z., Zeng D., Zhang Q. A dissemination model based on psychological theories in complex social networks // IEEE Transactions on Cognitive and Developmental Systems. – 2021. – Vol. 14. – No. 2. – P. 519–531. https://doi.org/10.1109/TCDS.2021.3052824.

22 Moscato V., Picariello A., Sperlí G. Community detection based on game theory // Engineering Applications of Artificial Intelligence. – 2019. – Vol. 85. – P. 773–782. https://doi.org/10.1016/j.engappai.2019.08.003.

23 Plekhanov D., Franke H., Netland T.H. Digital transformation: A review and research agenda // European Management Journal. – 2023. – Vol. 41. – No. 6. – P. 821–844. https://doi.org/10.1016/j.emj.2022.09.007.

REFERENCES

1 Wang J., Yang Y., Liu Q., Fang Z., Sun S., Xu Y. An empirical study of user engagement in influencer marketing on Weibo and WeChat, IEEE Transactions on Computational Social Systems, 10, 3228–3240 (2023). https://doi.org/10.1109/TCSS.2022.3204177.

2 Sun B., Al-Bayaty R., Huang Q., Wu D.O. Game theoretical approach for non-overlapping community detection. 2019 5th International Conference on Big Data Computing and Communications, 2019, pp. 222–230. https://doi.org/10.26599/TST.2020.9010017.

3 Bruning P.F., Alge B.J., Lin H.-C. Social networks and social media: Understanding and managing influence vulnerability in a connected society, Business Horizons, 63 (6), 749–761 (2020). https://doi.org/10.1016/j.bushor.2020.07.007.

4 Huang D., Tan X., Chen N., Fan Z. A memetic algorithm for solving the robust influence maximization problem on complex networks against structural failures, Sensors, 22 (6), 2191 (2022). https://doi.org/10.3390/s22062191.

5 Peng Y., Bai X. Identifying social tipping point through perceived peer effect, Environmental Innovation and Societal Transitions, 51, 2367–2382 (2024). https://doi.org/10.1016/j.eist.2024.100847.

6 Liu Y., Bao Z., Zhang Z., Tang D., Xiong F. Information cascades prediction with attention neural network, Human-centric Computing and Information Sciences, 10 (2020). https://doi.org/10.1186/s13673-020-00218-w.

7 Rangnani S., Devi V.S. Predicting potential retweeters for a microblog on Twitter, Intelligent and Evolutionary Systems, 5, 1–5 (2016). https://doi.org/10.1007/978-3-319-27000-5_14.

8 Qiang Z., Pasiliao E., Zheng Q. Model-based learning of information diffusion in social media networks, Applied Network Science, 4 (1), 1–16 (2019). https://doi.org/10.1007/s41109-019-0215-3.

9 Zhang L., Li K., Liu J. An information diffusion model based on explosion shock wave theory on online social networks, Applied Sciences, 11, 9996 (2021). https://doi.org/10.3390/app11219996.

10 Bourigault S., Lagnier C., Lamprier S., Denoyer L., Gallinari P. Learning social network embeddings for predicting information diffusion Proceedings of the 7th ACM International Conference on Web Search and Data Mining (WSDM '14), 2014, pp. 393–402. https://doi.org/10.1145/2556195.2556216.

11 Newman M.E.J. The structure and function of complex networks, SIAM Review, 45, 167–256 (2003). https://doi.org/10.1137/S00361445034248.

12 Tsai J., Nguyen T., Tambe M. Security games for controlling contagion, Proceedings of the AAAI Conference on Artificial Intelligence, 2021, vol. 26, no.1, pp. 1464–1470. https://doi.org/10.1609/aaai.v26i1.8249.

13 Li Q., Du H., Li X.-Y. Influence of influence on social networks: Information propagation causes dynamic networks, Proceedings of the 2021 7th International Conference on Big Data Computing and Communications (BigCom), 2021, pp. 278–285. https://doi.org/10.1109/BigCom53800.2021.00016.

14 Podlipskaia O. Determining effective strategies for information warfare in consolidated and polarized populations, Proceedings of the IEEE Conference on Machine Learning and Systems, 2022, pp. 1–5. https://doi.org/10.1109/MLSD55143.2022.9934658.

15 Li T., Zhao Y., Zhu Q. The role of information structures in game-theoretic MAL, Annual Reviews in Control, 53, 296–314 (2022). https://doi.org/10.1016/j.arcontrol.2022.03.003.

16 Ganai A.H., Hashmy R., Khanday H.A. Finding information diffusion's seed nodes in online social networks using a special degree centrality, SN Computer Science, 5, 333 (2024). https://doi.org/10.1007/s42979-024-02683-x.

17 Genschow O., Klomfar S., d'Haene I., Brass M. Mimicking and anticipating others' actions is linked to social information processing, PLoS One, 13 (3), e0193743 (2018). https://doi.org/10.1371/journal.pone.0193743.

18 Papadopoulou O., Makedas T., Apostolidis L., Poldi F., Papadopoulos S., Kompatsiaris I. MeVer NetworkX: Network analysis and visualization for tracing disinformation, Future Internet, 14 (5), 147 (2022). https://doi.org/10.3390/fi14050147.

19 Iqbal S., Arif T., Malik M., Sheikh A. Browser simulation-based crawler for online social network profile extraction, International Journal of Web Based Communities, 16, 321–342 (2020). https://doi.org/10.1504/IJWBC.2020.111377.

20 O'Neil D., Petty M. Heuristic methods for synthesizing realistic social networks based on personality compatibility, Applied Network Science, 4, 141–158 (2019). https://doi.org/10.1007/s41109-019-0117-4.

21 Luo T., Cao Z., Zeng D., Zhang Q. A dissemination model based on psychological theories in complex social networks, IEEE Transactions on Cognitive and Developmental Systems, 14 (2), 519–531 (2021). https://doi.org/10.1109/TCDS.2021.3052824.

22 Moscato V., Picariello A., Sperlí G. Community detection based on game theory, Engineering Applications of Artificial Intelligence, 85, 773–782 (2019). https://doi.org/10.1016/j.engappai.2019.08.003.

23 Plekhanov D., Franke H., Netland T.H. Digital transformation: A review and research agenda, European Management Journal, 41 (6), 821–844 (2023). https://doi.org/10.1016/j.emj.2022.09.007.

[1]*Молдабаев Д.А.,
магистрант, ORCID ID: 0000-0001-8389-2953,
*e-mail: d_moldabayev@kbtu.kz
[1]Тинал М.Б.,
магистрант, ORCID ID: 0000-0002-5503-0077,
e-mail: m_tinal@kbtu.kz
[1]Картбаев А.Ж.
PhD, ORCID ID: 0000-0003-0592-5865,
e-mail: a.kartbayev@gmail.com

[1]Қазақстан-Британ техникалық университеті, 050000, Алматы қ., Қазақстан

ОЙЫН ТЕОРИЯСЫНЫҢ ӘДІСТЕРІ НЕГІЗІНДЕ ӘЛЕУМЕТТІК ЖЕЛІДЕГІ АҚПАРАТТЫҚ ҚАРСЫ ӘРЕКЕТ МОДЕЛЬДЕРІНІҢ ПРАКТИКАЛЫҚ ТӘСІЛДЕРІН ӘЗІРЛЕУ

Аңдатпа

Бұл зерттеу пайдаланушылар арасындағы ақпараттық қақтығыс жағдайында әлеуметтік желідегі өзара әрекеттесу динамикасын талдайды. Зерттеуде ойын теориясы мен ықтималдық әдістеріне негізделген қақтығыстарды модельдеудің симуляциялық тәсілі ұсынылады. Сонымен қатар, зерттеу жұмысы желінің

күйін динамикалық бақылау, қадағалау және жаңарту әдісін ұсынады. Бұл инновациялық тәсіл ақпараттық қақтығыстарды екі ойыншының өзара іс-қимылы ретінде модельдейді, мұндағы негізгі мақсат — мүмкіндігінше көп желі түйіндерін басқару. Ойын теориясын қолдана отырып, біз Facebook Researcher ашық деректер жиынтығы мен қазақстандық сегменттің ағымдағы желілік жағдайына негізделген, әрбір ойыншының шешім қабылдау стратегиясын бейімдеуге мүмкіндік беретін алгоритм тұжырымдадық. Ұсынылған желі күйін динамикалық бақылау әдісі ресурстарды тұтынуды едәуір азайтып, есептеу тиімділігін арттыруға септігін тигізеді. Басқа әдістермен салыстырғанда жүргізілген есептік сынақтар ұсынылып отырған тәсілдің практикалық құндылығын дәлелдеді. Бұл әдістің икемділігі мен тиімділігі оны ақпараттық және аналитикалық жүйелердегі мәселелердің кең ауқымын шешуге арналған болашағы зор құралға айналдырады.

Тірек сөздер: ойын теориясы, стратегияға бейімделу, әлеуметтік желі, ақпараттық қақтығыс, модельдеу алгоритмі, ықтималдық көзқарас, аналитикалық жүйелер.

[1]*Молдабаев Д.А.,
магистрант, ORCID ID: 0000-0001-8389-2953,
*e-mail: d_moldabayev@kbtu.kz
[1]Тинал М.Б.,
магистрант, ORCID ID: 0000-0002-5503-0077,
e-mail: m_tinal@kbtu.kz
[1]Картбаев А.Ж.
PhD, ORCID ID: 0000-0003-0592-5865,
e-mail: a.kartbayev@gmail.com

[1]Казахстанско-Британский технический университет, г. Алматы, Казахстан

РАЗРАБОТКА ПРИКЛАДНОГО ПОДХОДА К МОДЕЛИРОВАНИЮ ИНФОРМАЦИОННОГО ПРОТИВОСТОЯНИЯ В СОЦИАЛЬНЫХ СЕТЯХ НА ОСНОВЕ МЕТОДОВ ТЕОРИИ ИГР

Аннотация

В данной работе исследуется динамика социальных сетей в контексте информационного противоборства между пользователями. В работе представлен новый способ моделирования информационного противоборства в социальных сетях, основанный на теоретико-игровых и вероятностных подходах. Кроме того, в статье предлагается метод динамического наблюдения, отслеживания и обновления состояния сети. Этот инновационный метод концептуализирует информационные конфликты как игру для двух игроков, целью которой является контроль как можно большего числа узлов сети. Применяя теорию игр, мы разработали эффективный алгоритм адаптации стратегий, который позволяет каждому игроку модифицировать свое принятие решений на основе открытого набора данных Facebook Researcher (а именно его казахстанского сегмента) и текущих условий сети. Метод динамического отслеживания состояния сети, представленный в данном исследовании, приводит к значительному снижению использования ресурсов и улучшению вычислительной эффективности. Сравнительные вычислительные тесты с другими методологиями демонстрируют практическую ценность нашего подхода. Гибкость и эффективность предложенного метода делают его перспективным инструментом для решения широкого спектра задач в информационных и аналитических системах.

Ключевые слова: теория игр, адаптация стратегий, социальные сети, информационный конфликт, алгоритм моделирования, вероятностный подход, аналитические системы.

Article submission date: 24.04.2024