The Scientific Temper (2023) Vol. 14 (4): 1537-1543

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.69

https://scientifictemper.com/

RESEARCH ARTICLE

# Influence node analysis based on neighborhood influence vote rank method in social network

**Sreenath M.V. Reddy[1*], D. Annapurna[1], Anand Narasimhamurthy[2]**

## Abstract

Social networks are used for various purposes like advertising, product launches, sentiment analysis, opinion mining, and event detection etc. Terrorist targets social network users to spread the terrorism. Influence analysis is used in social networks to find the influence of users and the impact of the messages, mainly for advertising. In this research, the neighborhood Influence – Vote Rank (NI-VR) method is proposed to analyze the terrorism and social network datasets temporally to find the influence node in social networks. The global terrorism dataset (GTD) was used to analyze the terrorism activity and temporal analysis on social network data to find the influence node. The neighborhood node influence is measured and considered in the social network data to effectively find the influence node. The nodes' vote score and vote ability were measured to rank the nodes based on influence. The neighborhood influence is measured to update the vote score and vote ability based on influence value. The neighborhood influence method is applied to rank the node has the advantage of analyzing the probability of affected nodes and recover nodes that help to effectively find the influence nodes. The outcomes illustrate that the proposed NI-VR achieved a maximum spread influence of 843 and the existing Greedy method has a higher spread influence of 840 in influence node analysis.

**Keywords**: Global terrorism dataset, Neighborhood influence–Vote rank, Neighborhood node influence, Social networks, Vote score.

## Introduction

Increases in the usage of social networks such as Facebook and Twitter increase the amount of information exchanged in form of intentions, emotions, sentiments, and opinions. This information reflects aptitude and affiliations towards and policy, event, and entity (Giavazzi *et al.*, 2023). Social network has become the largest and most influential web component during the last decade and is not limited in social sciences and sociology. Users' relations can be studied for engineering, economics, and political science. Several studies were carried out on social network information to track the terrorist activity in social networks and the connections (Spelta *et al.*, 2023). Social networks have been targets for terrorists to direct contact with their target audience and spread or recruit terrorists (Wolfowicz *et al.*, 2021). Social media messages are short, imprecise, and don't provide insufficient information. Social media messages are present in unstructured format, spelling mistakes, ungrammatical construction, and abbreviations (Singh & Singh, 2021). Recently, social network analysis is used to analyze the relationship between organizations and people to analyze activities, sentiment analysis and dynamics that other circles networks being involved in (Castaño-Pulgarín *et al.*, 2021). The influence maximization method is the process of finding K-sized users subset based on seed value that leads to maximum influence spread in social networks (Rawat *et al.*, 2022). The terrorist organization has a different strategy and doesn't provide full information about their situation. Learning models in adaptive processes is likely to provide higher efficiency in the model of the behavior (Babu & Kanaga, 2022).

Since the beginning of written history, terrorism has existed (Aldera *et al.*, 2021), a thing that stirs up those days to the core is terrorism. Governments start to worry about it, and academics start to be interested in the subject (El Barachi *et al.*, 2021). The security of civilization is under jeopardy due

[1]Department of Computer Science and Engineering, PESIT, Bangalore, India

[2]Department of Computer Science and Engineering, INSOFE, Bengaluru, India

***Corresponding Author:** Sreenath M.V. Reddy, Department of Computer Science and Engineering, PESIT, Bangalore, India, E-Mail: sreenathmv.pes@outlook.com

**How to cite this article:** Reddy, S.M.V., Annapurna, D., Narasimhamurthy, A. (2023). Influence node analysis based on neighborhood influence vote rank method in social network. The Scientific Temper, **14**(4):1537-1543.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.69

**Source of support:** Nil

**Conflict of interest:** None.



**Received:** 12/10/2023 **Accepted:** 17/11/2023 **Published:**27/12/2023

to the ease of information exchange and the accessibility of weapons of mass destruction to small terrorist organizations (KhosraviNik & Amer, 2022). The military-led structured war is no longer the appropriate strategy for the fight against terrorism (Piazza, 2022). Microblogging tools like Twitter, which have millions of users worldwide, are one of the new Web 2.0 inventions. These kinds of applications developed into a platform for the exchange of ideas and information among users (Bright *et al.*, 2021). Twitter is an excellent source of information regarding how users perceive various terrorist organizations through analysis of their tweets, in addition to being helpful in tracking terrorism and identifying threats (Antonakaki *et al.*, 2021). The popularity of social media and the speed at which users share and receive information make data analysis even more crucial (Ahmed *et al.*, 2022). The unstructured content of tweets can be analyzed using text mining and sentiment analysis techniques, which can reveal hidden patterns for a variety of real-world scenarios (Ul Rehman *et al.*, 2021).

This paper is formulated as a literature review of the influence node analysis and terrorist prediction, which are given in section 2 and the explanation of proposed NI-VR method in section 3. The simulation setup of the proposed method implementation is given in section 4 and the experimental result of the proposed method is given in section 5. Finally, the conclusion is given in section 6.

### *Literature Survey*

Researchers use Social Network data to find the spreading of terrorism for counter-terrorist operations. The various influence analysis methods in the social networks were used to find the spreading of terrorism. Some of the notable researches in the finding the spreading of terrorism in the social network data were reviewed in this section.

To analyze digital diplomacy on Twitter, Khan *et al.* (2021) presented the public engagement model, commonly known as a social media analytics framework. The main themes of the ambassador's tweets were to respond to those tweets, and the kinds of issues that attracted more engagement over the course of two years were investigated using a text analytics approach. Further, presents a public engagement model (PEM) for social media communication by identifying three crucial elements that encourage online public involvement: self-disclosure, a positive outlook, and inquisitiveness. This is done by analyzing the content of the tweets even though the ambassador must still manage embassy matters as a country's representative.

For the purpose of predicting crime, Boukabous and Azizi (2022) used a hybrid sentiment analysis approach based on the bidirectional encoder representations from transformers. The deep learning model utilized in this study, BERT, is a hybrid approach that blends lexicon-based and deep learning techniques. Then, using a set of normal and crime-related lexicons, we used the lexicon-based strategy to label our Twitter dataset. Finally, we used the labeled dataset to train the BERT model. When it comes to these kinds of words, the model's performance suffers due to the challenge of analyzing and interpreting metaphorical, sardonic, and encrypted English expressions in the context of sentiment analysis. However, the suggested approach was still unable to handle these expressions.

In order to detect racism, xenophobia, and genderism in online social networks, Kaya and Alatas (2022) developed a new hybrid long short-term memory-recurrent neural network (LSTM-RNN) deep learning model. The purpose of this study is to develop a novel hybrid prediction model that can accurately and effectively identify remarks that are racist, xenophobic, and sexist when they are published in English on Twitter, a well-known social media network. The novel hybrid LSTM-RNN models that were suggested yielded better performance results for the detection of hate speech. The LSTM-RNN model produced more precise, efficient, and reliable findings and could be easily adjusted to address a wide range of additional social network and media issues even though this study's offensive language was frequently used to refer to abusive language.

By means of a hybrid LSTM-support vector machine (SVM) classification technique, Kiruthikaa and Thailambal (2022) created a dynamic lightweight recommendation system for social networking analysis. Both methods were used in the classification and training phases in this case. The weights gained from the penultimate network layer were used to build a feature vector for each vector in the training set of the statistical model of the LSTM neural network. Using an SVM classifier, the training phase was finished. For each vector that needs to be classified, the same stages are employed in the classification phases, and an embedding vector was created using the previously trained LSTM network. Last but not least, the SVM classifier provides predicted classes by combining the embedding vector with other classification features. However, learning the sentences and terms would have been easier if they had been in a lengthier text.

In the context of terrorist incidents, An *et al.* (2023) employed prediction and evolution of the influence of microblog entries. This study builds a prediction model of microblogging influence in terrorist scenarios using a classification process and uses the K-fold cross-validation to evaluate the prediction model to study the prediction and evolution of terrorist events. The research assists counterterrorism organizations in accurately and quickly predicting influential microblogs and taking preventative action in advance to lessen public anxiety brought on by terrorist acts. However, many users do not convey their viewpoints while sharing microblogs, making it challenging to grab other users' attention.

A classification technique based on mutual clustering coefficient and user profile information has been published

by Wani and Jabin (2022) to identify suspicious linkages within user communities. We may compare user profiles to determine how similar they are. In order for a user to independently evaluate the suggested links and filter their buddy list according to their preferences, service providers have used the proposed model to present to its members a list of problematic connections from their separate friend networks. Even though the suggested strategy has only been tested with Facebook users, it can still be used with a minor change on other social networking sites.

A framework for detection and integration of unstructured data of hate speech (FADOHS) on Facebook using sentiment and emotion analysis was created by Rodriguez *et al.* (2022). In order to make all social media service providers aware of how ubiquitous hate is on social media, the FADOHS combines data analysis and natural language processing techniques. Analyze recent posts and comments on these pages using sentiment and emotion analysis algorithms. Posts that were thought to contain dehumanizing language were screened before being sent to the clustering algorithm. In the end, hate-speech clustering was used to identify and classify information into various groups based on the level of expressed hatred utilizing hybrid approaches. Although it often cannot isolate the primary focus of chosen groups, the more posts that were looked at (mildly critical posts).

## Method

Here, the NI-VR is recommended to find the influence node in the social network data. The GTD is used to evaluate the efficiency of the NI-VR and the existing Vote Rank method. The graph was constructed based on the input data and influence spread was measured. Vote score and vote ability are measured on the nodes to analyze the influences of the nodes. Neighborhood influence is measured and used to update the vote score and vote ability. The influence node is measured based on neighborhood influence on the analysis. The overview of the proposed NI-VR method is displayed in Figure 1.

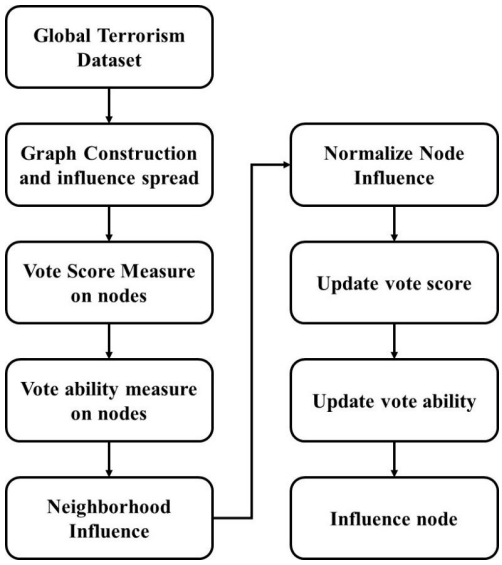


**Figure 1:** The overview of the proposed Neighborhood Influence Vote Rank method

### *Graph Construction and Influence spread*

Influence spread is a measure of the influence diffusion process in expected active nodes for specified node-set $S$ (seeds) and initiated specific diffusion model. The influence spread is denoted as $\sigma(S)$ for a given node-set $S$. In simple manner, influence maximization is a measure of influence spread $\sigma(S)$ maximum based on node set $S$.

Influence maximization is considered as a constrained optimization issue and this is described below:

Consider a graph $G = (V, E)$ and a number $K$ $(0 < K < |V|)$, where node-set is denoted as $S = \{s_1, s_2, \ldots s_K\}$, an initial node is denoted as $K$ that spreads the influence in a definite diffusion model, therefore, concluding influence spread $\sigma(S)$ is higher. The optimization issue is defined in equation (1).

$$G = \begin{cases} S = argmax\ \sigma(S) \\ subject\ to |S| = K \end{cases} \quad (1)$$

### *VoteRank*

VoteRank centrality applies voting schemes notion to find multiple spreader in social network data (Liu et al., 2021). Every vertex $v \in V$ is related to tuple $(S_v, Va_v)$, where vertex $v$ voting score is denoted as $S_v$, and vertex $v$ voting ability is denoted as $Va_v$. The adjacent neighbors is used to measure the voting score $S_v$ and all its neighbor's voting ability is used to compute vote measure, as given in equation (2).

$$S_v = \sum_{i \in N(v)} Va_i \quad (2)$$

Where $v$ neighbors are denoted as $N(v)$. VoteRank centrality follows four stages:

*Initialization phase*

Tuple $(S_v, Va_v)$ is present for every vertex $v$ as (0, 1), i.e., each node voting ability is 1 and voting score is 0.

*Voting phase*

This stage proceeds voting, where each node $v$ immediate neighbors sum of voting abilities. The maximum vote of a node is set as a spreader in this cycle if it is not previously designated as a spreader. The selected node has been set with zero voting ability, that ensures the selected node not considered for further voting rounds.

*Update phase*

Selected spreader neighboring nodes is reduced in their voting abilities in the next iteration to select far apart position spreaders. Neighbor's voting ability is reduced of the elected spreader as $Va_v = Va_v - \delta$, (if $Va_v > \delta$, or 0), where $\delta = 1/\langle k \rangle$ and $\langle k \rangle$ are network nodes average degree.

*Iteration phase*

Until $c$ nodes are selected as a spreader, repeat steps (ii) and (iii). VoteRank centrality is more accurate than K-shell, H-index, Cluster Rank, and Degree. Vote scheme is selected based on a set of spreaders when nodes get an equal vote from their neighbor and node degree is a significant standard to be nominated. Node with a lesser degree in network core also plays a dynamic part in permitting the data (Kumar et al., 2021).

### *Neighborhood Influence-based Vote Rank*

Vote Rank based centrality method based on seed nodes was introduced to find the influence nodes. A voting scheme is applied to select a set of spreaders where the neighbor node vote and each node has the same voting ability. Every node needs to be dissimilar based on network topological location. NCVoteRank centrality is VoteRank with coreness that uses the coreness range of neighbors to voting. Every node $v \in V$ is related to tuple $(S_v, Va_v)$, where node $v$ voting score and ability is denoted as $S_v$ and $Va_v$ respectively. Voting ability $(Va_v)$ denotes the vote of node $v$ for its neighbors. Adjacent neighbors' voting score is $S_v$ is computed based on voting ability, as given in equation (4), $S_v = \sum_{i \in N(v)} Va_i$ , where node $v$ adjacent neighbors are denoted as $N(v)$.

NCVoteRank has four stages

Initialization Phase: Tuple $(S_v, Va_v)$ as (0, 1) is applied in each node $v$, each node voting ability is 1 and voting score is 0.

*Voting phase*

Network core nodes affect information diffusion and the Neighborhood Coreness (NC) value is multiplied with each node voting ability. Each node $v$ gets a vote based on immediate neighbors of a sum of voting abilities, as given in equation (3).

$$S_v = \sum_{i \in N(v)} (Va_i \times NC(i) \times (1 - \theta) + Va_i \times \theta) \quad (3)$$

Where controlling parameter is denoted as $\theta$ that varies in between 0 and 1, and vertex normalized neighborhood coreness $i$, where node $v$ immediate neighbor is vertex $i$, neighborhood coreness value is normalized to solve scaling issues due to greatly varying magnitudes. Standard scores are used for normalization and variable $x$ standard score in the list is in equation (4).

$$\overline{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (4)$$

Where minimum and maximum values are denoted as $x_{min}$ and $x_{max}$, respectively, If $\theta = 0$, carry out equation (5).

$$S_v = \sum_{i \in N(v)} Va_i \times NC(i) \quad (5)$$

Node $v$ vote score $(S_v)$ is equivalent to the voting ability of products summation and neighborhood coreness of its direct neighbors, as given in equation (5). Node score varies between two measures: (i) Neighbors sum of the voting ability, (ii) Neighborhood coreness sum of the product of voting ability and direct neighbors. In this round, a node with the maximum vote is considered as a spreader, if it is not previously selected. The selected node is not participating in the voting round based on the configuration of its voting ability as 0.

*Update Phase*

Spreaders is needed topic from diverse positions to achieve network information coverage. This influence of its neighbors increases to two hops if a node is set as a spreader. A $\delta$ factor is reducing the all-neighbor voting ability from selected spreader of distance two nodes. Neighbor nodes of updated voting ability is denoted as $Va_v$, as given in equation (6).

$$Va_v = \begin{cases} Va_v - \delta & if\ Va_v - \delta > 0 \\ otherwise \end{cases} \quad (6)$$

Where $\delta = 1/kd$.

Network nodes of average degree are denoted as $k$ and selected nodes' distance is denoted as $d$ and two units' distance of updating neighbor (i.e., $d = 1, 2$). If the node is set as a spreader, neighbors in distance two voting ability are updated based on equation (6). No random selection of $d$ value and reduction are carried out for up to distance two all updating neighbors. This ensures the spreaders selected from network diverse positions.

*Iteration phase*

Until $c$ nodes are selected as a spreader, repeat steps (ii) and (iii) and $c$ is constant.

*Spreading model*

The stochastic susceptible infected recovery (SIR) mode is used in this model (Noor *et al*., 2022; Dai *et al*., 2022) to estimate the proposed model performance. Spreaders list or network nodes subset is provided as input to a user to measure recovery probability ($\gamma$) and infection probability ($\beta$). The neighbor node sends information to the nodes in susceptible. At any instant of time, infected nodes carry information and recovered denotes the node sends information to the susceptible node. The $\gamma$ is set as one that susceptible nodes transmitted information of infected nodes send to recovered state in subsequent time stamp $t + 1$ onwards and doesn't send the information again i.e., nodes not infected. The infection probability value is selected and better over the epidemic threshold ($\beta^{th}$). The influential spreader input list is considered infected at $t = 0$ and neighbors with probability $\beta$ are infected by each successive timestamp infected nodes i.e., randomly $p$, neighbor nodes are selected. The $p$ integer is below or equivalent to $\beta$ times the overall neighbors of the infected node. The whole process is required to run several times due to the presence of model randomness and simulation is carried out for results average.

*Algorithm: Proposed Neighbor Influence Vote Rank (NI-VR)*

**Input:** Global Terrorism Dataset
**Output:** Influenced node

Construct the Graph based on Input data
Measure voting score of vertex $S_v$
Measure voting ability of vertex $Va_v$
Initiate tuples $(S_v, Va_v)$
For select spreader node $c$
    Measure Neighborhood Influence $(NI)$
    Measure Voting ability of Neighbors
    For vertex $i$ in an immediate neighbor of node $v$
        Normalize neighbor node influence $NI(i)$
    End
    Update vote score
    Update voting ability
End
Developed SIR spreader model
Measure infection probability $\beta$
Measure recovery probability $\gamma$
Find influence score based on vote score

### *Simulation Setup*

The execution particulars of the proposed process such as dataset, parameter settings, metrics, and system configuration, were given in this section.

### *Dataset*

The Global Terrorism Database (GTD) consists of various terrorist attacks in the year 1970 to 2017 (Santos *et al.*, 2019; Hu *et al.*, 2019; Gao *et al.*, 2017; Husain *et al.*, 2020). The database consists of domestic and international terrorist incidents and consists of 180,000 attacks. The record is preserved by the study of terrorism and responses to terrorism (START), headquartered on the University of Maryland. The database is present in https://www.kaggle.com/START-UMD/gtd.

### *Parameter settings*

*Metrics*

The proposed and existing methods were evaluated using the metrics of expected influence spread and computation time. The existing methods such as Greedy and vote rank were compared with the behavior of the proposed NI-VR.

*System configuration*

The proposed NI-VR is executed in the structure comprised of an Intel i9 processor, 128 GB of RAM and 22 GB Graphics card. Python 3.7 is utilized to execute the NI-VR method. The proposed and existing methods were implemented in the same environment and data.

## Results

Influence node detection in terrorism spread based on terrorist data helps the police to prevent terrorist attacks. The existing methods involve the prediction of terrorist attacks based on the terrorist data. Here, the NI-VR is suggested to detect the influence node to prevent terrorism spread. The GTD was used in this method to detect the influence node in the terrorism spread. This section discusses

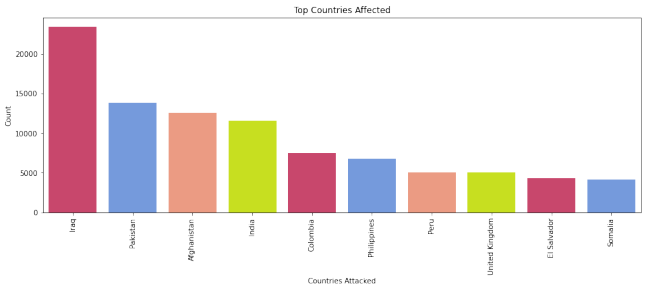


**Figure 2:** Top affected countries in database

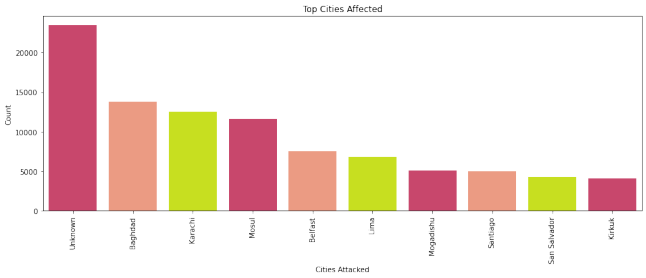


**Figure 3:** Top affected cities in the database

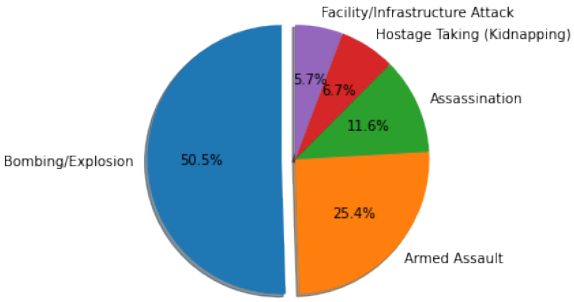


**Figure 4:** Types of attacks in the database

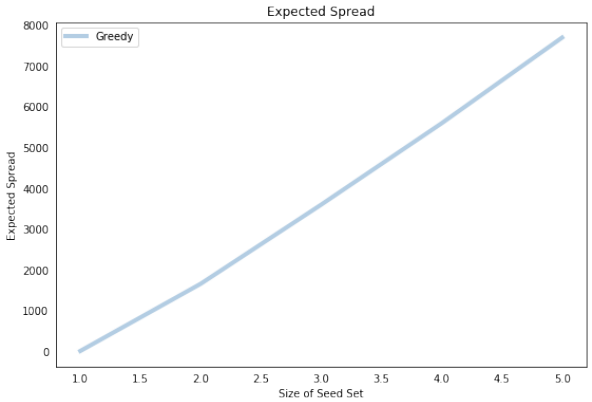


**Figure 5:** Expected spread of NI-VR

the data analysis and results analysis of the proposed NI-VR and existing methods.

The top affected countries and top affected cities in GTD are displayed individually in Figures 2 and 3. Figure 2 displays that Iraq country has the most terrorist attack in the database and Figure 3 shows that Baghdad city has the

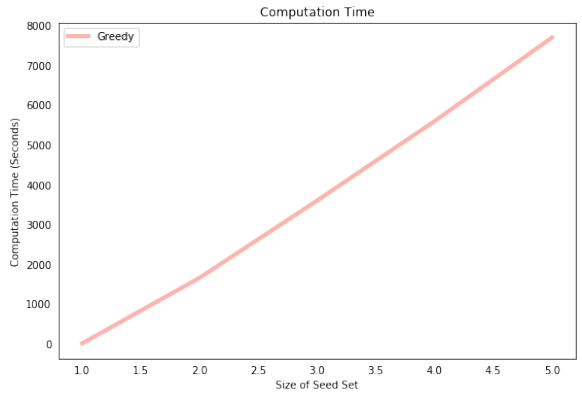


**Figure 6:** The computation time of NI-VR

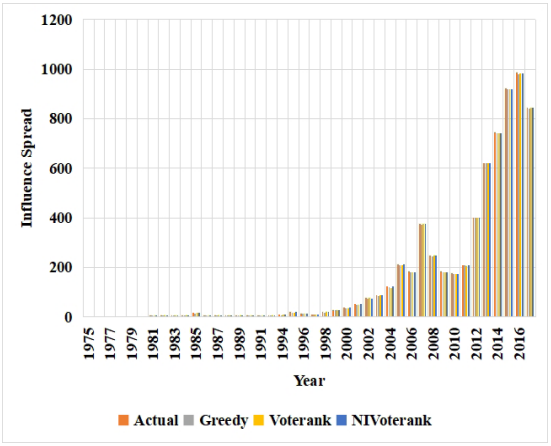


**Figure 7:** Influence analysis of proposed NI-VR method on various Year

most terrorist attack in the data. Figure 3 displays that most of the terrorist attacks in the cities are unknown.

The types of attacks in the database and their percentage in overall attack types are shown in Figure 4. The Bombing/ Explosion is the common terrorist attack in the database and armed assault is the second common terrorist attack in the database. NI-VR expected spread of influence based on various seed sets is displayed in Figure 5.

The study presents that increases in the seed set to increase the influence spread in the method. The proposed NI-VR method has the advantages of analyzing the influence node and update the vote ability and vote score. The spread is linear because the communication between the events is uniform and not biased with weight. The computation time of the NI-VR method for analyzing the influence node for various seed sets as shown in Figure 6.

The computation time of the proposed NI-VR method for various seed size due to the assumption that communication between the events is uniform and not biased with weights. The proposed NI-VR method has the advantage of update the vote score and vote ability based on the influence node. The influence analysis of the proposed NI-VR method and existing Greedy and Voterank method for various years is exposed in Figure 7.

The results display that the NI-VR has maximum improvement in the influence study compared to Greedy and Voterank. The proposed NI-VR method has the advantage of updating the vote score and vote ability based on the influence node.

## Conclusion

Terrorism spreading detection in social networks helps the police to take necessary action to prevent terrorist attacks. Terrorist targets social network users to spread terrorism, which needs to be detected to prevent terrorist attacks. Few researches were carried out to detect the terrorism spreading in a social network. Here, the NI-VR is recommended to detect the influence node for terrorism spread. The GTD was used to analyze the proposed NI-VR method and Voterank method in the influence analysis. The proposed NI-VR method has the advantage of update the vote score and vote ability based on the influence node. The outcome displays that the proposed NI-VR has better performance when contrasted with the conventional Vote rank technique. The future work of the proposed NI-VR method involves applying the machine learning technique to predict the terrorist attack.

## Author Contributions

Sreenath Marimakalapalli Venkatarama Reddy: Data curation; Conceptualization; Resources; Methodology; Resources; Formal analysis; Roles/Writing - original draft.

D. Annapurna: Visualization; Software; Investigation; Validation; Supervision; Writing - review & editing; Project administration.

Anand Narasimhamurthy: Resources; Formal analysis; Supervision; Writing - review & editing.

All authors have read and approved the final manuscript.

Data Availability: The datasets generated during and/or analysed during the current study are available in the [Global Terrorism Database (GTD)] repository, [LINK] = https://www.kaggle.com/START-UMD/gtd.

## References

Ahmed, A. A. A., Agarwal, S., Kurniawan, I. G. A., Anantadjaya, S. P. D., & Krishnan, C. (2022). Business boosting through sentiment analysis using Artificial Intelligence approach. International Journal of System Assurance Engineering and Management, 13(Suppl 1), 699-709. https://doi.org/10.1007/s13198-021-01594-x

Aldera, S., Emam, A., Al-Qurishi, M., Alrubaian, M., & Alothaim, A. (2021). Online extremism detection in textual content: a systematic literature review. IEEE Access, 9, 42384-42396. DOI: 10.1109/ACCESS.2021.3064178

An, L., Han, Y., Yi, X., Li, G., & Yu, C. (2023). Prediction and evolution of the influence of microblog entries in the context of terrorist events. Social Science Computer Review, 41(1), 64-82. https://doi.org/10.1177/08944393211029193

Antonakaki, D., Fragopoulou, P., & Ioannidis, S. (2021). A survey of Twitter research: Data model, graph structure, sentiment analysis and attacks. Expert Systems with Applications, 164,

114006. https://doi.org/10.1016/j.eswa.2020.114006

Babu, N. V., & Kanaga, E. G. M. (2022). Sentiment analysis in social media data for depression detection using artificial intelligence: a review. SN Computer Science, 3, 74. https://doi.org/10.1007/s42979-021-00958-1

Boukabous, M., & Azizi, M. (2022). Crime prediction using a hybrid sentiment analysis approach based on the bidirectional encoder representations from transformers. Indones. J. Electr. Eng. Comput. Sci, 25(2), 1131-1139. DOI: http://doi.org/10.11591/ijeecs.v25.i2.pp1131-1139

Bright, D., Brewer, R., & Morselli, C. (2021). Using social network analysis to study crime: Navigating the challenges of criminal justice records. Social Networks, 66, 50-64. https://doi.org/10.1016/j.socnet.2021.01.006

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021). Internet, social media and online hate speech. Systematic review. Aggression and Violent Behavior, 58, 101608. https://doi.org/10.1016/j.avb.2021.101608

Dai, Y., Zhou, B., Jiang, D., & Hayat, T. (2022). Stationary distribution and density function analysis of stochastic susceptible-vaccinated-infected-recovered (SVIR) epidemic model with vaccination of newborns. Mathematical Methods in the Applied Sciences, 45(7), 3401-3416. https://doi.org/10.1002/mma.7986

El Barachi, M., AlKhatib, M., Mathew, S., & Oroumchian, F. (2021). A novel sentiment analysis framework for monitoring the evolving public opinion in real-time: Case study on climate change. Journal of Cleaner Production, 312, 127820. https://doi.org/10.1016/j.jclepro.2021.127820

Gao, J., Fang, P., & Liu, F. (2017). Empirical scaling law connecting persistence and severity of global terrorism. Physica A: Statistical Mechanics and its Applications, 482, 74-86. https://doi.org/10.1016/j.physa.2017.04.032

Giavazzi, F., Iglhaut, F., Lemoli, G., & Rubera, G. (2023). Terrorist Attacks, Cultural Incidents, and the Vote for Radical Parties: Analyzing Text from Twitter. American Journal of Political Science. (Online Version of Record before inclusion in an issue).

Hu, X., Lai, F., Chen, G., Zou, R., & Feng, Q. (2019). Quantitative Research on Global Terrorist Attacks and Terrorist Attack Classification. Sustainability, 11(5), 1487. https://doi.org/10.3390/su11051487

Husain, S. S., Sharma, K., Kukreti, V., & Chakraborti, A. (2020). Identifying the global terror hubs and vulnerable motifs using complex network dynamics. Physica A: Statistical Mechanics and Its Applications, 540, 123113. https://doi.org/10.1016/j.physa.2019.123113

Kaya, S., & Alatas, B. (2022). A New Hybrid LSTM-RNN Deep Learning Based Racism, Xenomy, and Genderism Detection Model in Online Social Network. International Journal of Advanced Networking and Applications, 14(2), 5318-5328.

Khan, M. L., Ittefaq, M., Pantoja, Y. I. M., Raziq, M. M., & Malik, A. (2021). Public engagement model to analyze digital diplomacy on Twitter: A social media analytics framework. International Journal of Communication, 15, 1741-1769.

KhosraviNik, M., & Amer, M. (2022). Social media and terrorism discourse: the Islamic State's (IS) social media discursive content and practices. Critical Discourse Studies, 19(2), 124-143. https://doi.org/10.1080/17405904.2020.1835684

Kiruthika, N. S., & Thailambal, D. G. (2022). Dynamic light weight recommendation system for social networking analysis using a hybrid LSTM-SVM classifier algorithm. Optical Memory and Neural Networks, 31(1), 59-75. https://doi.org/10.3103/S1060992X2201009X

Kumar, S., Singhla, L., Jindal, K., Grover, K., & Panda, B. S. (2021). IM-ELPR: Influence maximization in social networks using label propagation based community structure. Applied Intelligence, 51(11), 7647-7665. https://doi.org/10.1007/s10489-021-02266-w

Liu, P., Li, L., Fang, S., & Yao, Y. (2021). Identifying influential nodes in social networks: A voting approach. Chaos, Solitons & Fractals, 152, 111309. https://doi.org/10.1016/j.chaos.2021.111309

Noor, M. A., Raza, A., Arif, M. S., Rafiq, M., Nisar, K. S., Khan, I., & Abdelwahab, S. F. (2022). Non-standard computational analysis of the stochastic COVID-19 pandemic model: An application of computational biology. Alexandria Engineering Journal, 61(1), 619-630. https://doi.org/10.1016/j.aej.2021.06.039

Piazza, J. A. (2022). Fake news: the effects of social media disinformation on domestic terrorism. Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide, 15(1), 55-77. https://doi.org/10.1080/17467586.2021.1895263

Rawat, R., Mahor, V., Garg, B., Telang, S., Pachlasiya, K., Kumar, A., Shukla, S. K., & Kuliha, M. (2022). Analyzing newspaper articles for text-related data for finding vulnerable posts over the internet that are linked to terrorist activities. International Journal of Information Security and Privacy (IJISP), 16(1), 1-14. DOI: 10.4018/IJISP.285581

Rodriguez, A., Chen, Y. L., & Argueta, C. (2022). FADOHS: framework for detection and integration of unstructured data of hate speech on facebook using sentiment and emotion analysis. IEEE Access, 10, 22400-22419. DOI: 10.1109/ACCESS.2022.3151098

Santos, C., El Zahran, T., Weiland, J., Anwar, M., & Schier, J. (2019). Characterizing chemical terrorism incidents collected by the global terrorism database, 1970-2015. Prehospital and disaster medicine, 34(4), 385-392. DOI: https://doi.org/10.1017/S1049023X19004539

Singh, L. G., & Singh, S. R. (2021). Empirical study of sentiment analysis tools and techniques on societal topics. Journal of Intelligent Information Systems, 56(2), 379-407. https://doi.org/10.1007/s10844-020-00616-7

Spelta, A., Pecora, N., & Pagnottoni, P. (2023). Assessing harmfulness and vulnerability in global bipartite networks of terrorist-target relationships. Social Networks, 72, 22-34. https://doi.org/10.1016/j.socnet.2022.08.003

Ul Rehman, Z., Abbas, S., Khan, M. A., Mustafa, G., Fayyaz, H., Hanif, M., & Saeed, M. A. (2021). Understanding the Language of ISIS: An Empirical Approach to Detect Radical Content on Twitter Using Machine Learning. Computers, Materials & Continua, 66(2), 1075-1090. https://doi.org/10.32604/cmc.2020.012770

Wani, M. A., & Jabin, S. (2022). Mutual clustering coefficient-based suspicious-link detection approach for online social networks. Journal of King Saud University-Computer and Information Sciences, 34(2), 218-231. https://doi.org/10.1016/j.jksuci.2018.10.014

Wolfowicz, M., Perry, S., Hasisi, B., & Weisburd, D. (2021). Faces of radicalism: Differentiating between violent and non-violent radicals by their social media profiles. Computers in Human Behavior, 116, 106646. https://doi.org/10.1016/j.chb.2020.106646