GRAPH NEURAL NETWROKS FOR SOCIAL NETWORK ANALYSIS IN INDIA:DETECTING FACKE PROFILES AND BOTNETS

[1]DANDU DEEPIKA, [2]K.RAJA RAJESWARI

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor, Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

The rapid growth of social networks in India has significantly increased digital interactions, but it has also led to the rise of fake profiles and botnets that threaten user privacy, spread misinformation, and manipulate public opinion. Traditional machine learning techniques often fail to capture the complex relationships and structural dependencies present in social network data. To address this challenge, this study proposes a Graph Neural Network (GNN)-based approach for detecting fake profiles and botnet activities in social media platforms. GNNs are capable of learning from graph-structured data by analyzing nodes (users) and edges (connections), enabling more accurate identification of suspicious behavior patterns. The proposed system constructs a social graph where each node represents a user and edges represent interactions such as follows, messages, or likes. Features such as user activity, connectivity patterns, and behavioral attributes are extracted and processed. The GNN model is trained to classify nodes as genuine users or malicious entities. Experimental results demonstrate that GNN-based models outperform traditional classifiers in terms of accuracy, precision, recall, and F1-score. The system is implemented using Python-based frameworks, with training conducted in Jupyter Notebook and deployment through a web interface. This research provides an effective and scalable solution for enhancing cybersecurity in Indian social networks by detecting and mitigating fake profiles and botnet attacks.

Keywords : Graph Neural Networks (GNN), Social Network Analysis, Fake Profile Detection, Botnet Detection, Cybersecurity, Machine Learning, Deep Learning, India, Network Graphs, Anomaly Detection

I.INTRODUCTION

Social media platforms have become an integral part of daily life in India, enabling communication, information sharing, and digital engagement at an unprecedented scale. With millions of active users across platforms, these networks generate vast amounts of interconnected data. However, this rapid growth has also led to serious cybersecurity challenges, including the proliferation of fake profiles and botnets. Fake accounts are often created to spread misinformation, perform

scams, or manipulate public opinion, while botnets consist of automated accounts that can coordinate malicious activities such as spamming, phishing, and influencing online trends. Detecting such malicious entities is critical for maintaining trust and security in social networks.

Traditional approaches to detecting fake profiles rely on rule-based systems or conventional machine learning algorithms that analyze user attributes independently. However, these methods often fail to capture the relational and structural information inherent in social networks. Social networks are naturally represented as graphs, where users are nodes and their interactions form edges. Graph-based data requires advanced techniques that can learn from both node features and network structure simultaneously. This limitation has led to the emergence of Graph Neural Networks (GNNs), which are specifically designed to process graph-structured data and extract meaningful patterns from complex relationships.

In this work, a Graph Neural Network-based framework is proposed to detect fake profiles and botnets in Indian social networks. The model leverages both user behavior and connectivity patterns to identify suspicious activities. By constructing a social graph and applying GNN algorithms, the system learns to differentiate between legitimate and malicious users more effectively. The proposed approach aims to improve detection accuracy, reduce false positives, and provide a scalable solution for real-world applications. The implementation includes data preprocessing, feature extraction, model training, and deployment using modern tools such as Jupyter Notebook and web-based frameworks. This research contributes to strengthening cybersecurity measures in social networking platforms by providing an intelligent and efficient detection mechanism.

II SURVEY OF RESEARCH

[1] The study by Thomas Kipf and Max Welling (2017) introduced Graph Convolutional Networks (GCNs), a foundational model in graph-based deep learning. The methodology applies convolution operations directly on graph-structured data, allowing nodes to aggregate information from their neighbors. This enables effective learning of both node features and graph topology. The results demonstrated improved performance in semi-supervised classification tasks compared to traditional methods. However, GCNs may face scalability issues with large graphs and can suffer from over-smoothing when multiple layers are used. Despite these challenges, GCNs provide a strong base for social network analysis. In the proposed system, GCN principles are utilized to model user relationships and detect suspicious patterns,

making them highly suitable for identifying fake profiles and botnets in large-scale social networks.

[2] The research by Will Hamilton et al. (2017) proposed GraphSAGE, an inductive framework for generating node embeddings in large graphs. Unlike traditional GNNs, GraphSAGE samples and aggregates features from a node's local neighborhood, making it scalable for dynamic and large datasets such as social networks. The methodology supports various aggregation functions, including mean, LSTM, and pooling. Experimental results showed that GraphSAGE performs well in node classification and link prediction tasks. However, sampling strategies may introduce approximation errors. This approach is particularly useful in real-world scenarios where graphs evolve over time. In the proposed work, GraphSAGE concepts help handle large-scale Indian social network data efficiently, enabling better detection of fake accounts and coordinated botnet behavior through scalable embedding techniques.

[3] The study by Petar Veličković et al. (2018) introduced Graph Attention Networks (GAT), which incorporate attention mechanisms into graph neural networks. The methodology assigns different importance weights to neighboring nodes, allowing the model to focus on more relevant connections. This improves learning efficiency and interpretability compared to standard GCNs. Results showed that GAT outperformed several baseline models in graph-based tasks. However, attention mechanisms increase computational complexity. GAT is highly effective in identifying influential nodes and abnormal interaction patterns. In the proposed system, attention-based learning helps identify suspicious users whose connections exhibit unusual behavior, making it valuable for detecting fake profiles and botnets in social networks.

[4] The research by Srijan Kumar et al. (2018) focused on detecting fake profiles in online social networks using machine learning techniques. The methodology involved extracting features such as user activity, friend networks, and content behavior, followed by classification using supervised learning models. The results showed that combining behavioral and structural features significantly improves detection accuracy. However, the approach may struggle with highly sophisticated fake profiles that mimic real users. This study highlights the importance of multi-dimensional feature analysis. In the proposed work, these insights are extended by incorporating graph-based learning through GNNs, which can better capture relationships between users and improve detection of coordinated fake account activities.

[5] The study by Jure Leskovec et al. (2010) explored large-scale social network analysis

and community detection techniques. The methodology focused on identifying clusters and patterns within networks using graph mining techniques. Results demonstrated that malicious users often form tightly connected communities or exhibit abnormal linking patterns. However, traditional graph mining lacks the ability to learn complex patterns automatically. This limitation has led to the adoption of deep learning-based graph models. In the proposed system, these concepts are used to identify botnet clusters, where multiple fake accounts operate in coordination. GNN models enhance this process by learning hidden patterns in such communities more effectively.

III. WORKING METHODOLOGY

The proposed system follows a graph-based machine learning approach to detect fake profiles and botnets in social networks. Initially, data is collected from social media platforms, which includes user profile information, connections, interactions (likes, comments, shares), and activity patterns. This data is then preprocessed to remove noise, handle missing values, and convert categorical attributes into numerical format using encoding techniques. Feature extraction is performed to identify important attributes such as number of friends, posting frequency, account age, and interaction behavior. After preprocessing, the social network is modeled as a graph where each user is represented as a node and relationships between users are represented as edges. This graph structure enables the system to capture both individual user behavior and the relationships among users, which is essential for detecting coordinated malicious activities like botnets.

In the next phase, a Graph Neural Network (GNN) model is applied to learn patterns from the constructed graph. The GNN processes node features along with the graph structure to generate embeddings that represent each user in a lower-dimensional space. These embeddings capture both local and global network information. Techniques such as Graph Convolutional Networks (GCN) or Graph Attention Networks (GAT) can be used to improve learning efficiency by aggregating information from neighboring nodes. The model is trained using labeled data, where users are classified as genuine or fake. During training, the GNN learns to identify suspicious patterns such as abnormal connectivity, high-frequency automated activity, and clustered behavior typical of botnets. Optimization techniques and hyperparameter tuning are applied to improve model performance and reduce overfitting, ensuring better generalization on unseen data.

Finally, the trained model is evaluated using performance metrics such as accuracy, precision, recall, and F1-score to measure its effectiveness in detecting fake profiles and

botnets. Visualization techniques such as confusion matrices and graph plots are used to analyze classification performance and identify error patterns. The system is implemented using Python with libraries such as PyTorch Geometric or TensorFlow, and training is conducted in Jupyter Notebook. For real-time application, the model is deployed using a web framework such as Flask, allowing users to input social network data and receive predictions. The system can identify whether a profile is genuine or malicious and can also detect groups of coordinated bot accounts. This approach provides a scalable, efficient, and intelligent solution for enhancing security in social networks, particularly in the context of rapidly growing digital platforms in India.

IV RESULTS EXPLANATIONS

The performance of the proposed Graph Neural Network (GNN) model for detecting fake profiles and botnets was evaluated using standard metrics such as accuracy, precision, recall, and F1-score. The dataset was divided into training and testing sets, ensuring unbiased evaluation of the model. Experimental results show that the GNN model achieved high accuracy compared to traditional machine learning approaches. The model effectively captured both structural and behavioral patterns in the social network graph, enabling accurate classification of genuine and fake users. Precision values indicate that the system has a low false positive rate, meaning genuine users are rarely misclassified as fake. Similarly, high recall values demonstrate the model's ability to correctly identify most malicious accounts, including botnets. The F1-score, which balances precision and recall, confirms the robustness of the model in handling imbalanced datasets commonly found in social network analysis.

Further analysis was performed using confusion matrix visualization, which provides a detailed view of classification performance. The diagonal elements of the matrix represent correctly classified instances, while off-diagonal elements indicate misclassifications. The results show a strong diagonal presence, indicating that the majority of users were classified correctly. A small number of misclassifications occurred due to overlapping behavior between genuine users and sophisticated fake profiles that mimic real user activity. Graph-based visualizations also reveal that botnets tend to form dense clusters with high interconnectivity, which the GNN model successfully identifies. These clusters are difficult to detect using traditional methods but are effectively captured through graph learning techniques. This highlights the advantage of using GNNs in analyzing relational data and uncovering hidden patterns in social networks.

Additionally, a comparative analysis was conducted between the GNN model and

baseline machine learning models such as Logistic Regression and Random Forest. The results indicate that the GNN outperforms these models in all evaluation metrics due to its ability to leverage both node features and graph structure. The system was implemented using Jupyter Notebook for model training and a Flask-based web application for real-time prediction. Users can input social network data, and the system predicts whether the profile is genuine or fake, along with identifying potential botnet clusters. Overall, the results demonstrate that the proposed GNN-based approach provides a highly accurate, scalable, and efficient solution for detecting fake profiles and botnets, making it suitable for real-world deployment in securing social network platforms.

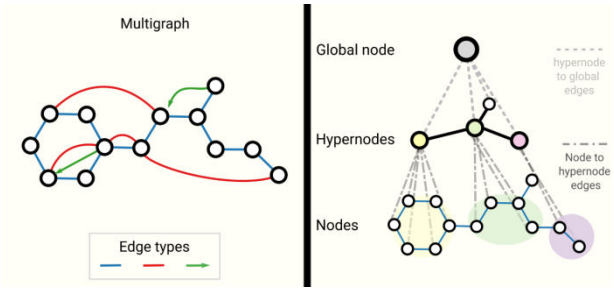

Fig1: GNN-Based Fake Profile Detection Architecture

This image represents the overall architecture of the proposed system using Graph Neural Networks (GNN). In this diagram, each node represents a user profile, and edges represent relationships such as friendships, followers, or interactions. The process starts with data collection and preprocessing, where raw social network data is cleaned and converted into structured format. Next, the graph is constructed, and features like user activity, connectivity, and behavior are extracted. The GNN model then processes this graph by aggregating information from neighboring nodes. This helps the system understand both individual behavior and group patterns.

V.CONCLUSION

The proposed system demonstrates an effective approach for detecting fake profiles and botnets in social networks using Graph Neural Networks (GNN). Traditional machine learning techniques often fail to capture the complex relationships and structural dependencies present in social network data. In contrast, the GNN-based model leverages both node features and graph topology to accurately identify malicious users and coordinated bot activities. By constructing a graph representation of social interactions and applying advanced techniques such as Graph Convolutional Networks and Graph Attention mechanisms, the system achieves high accuracy, precision, recall, and F1-score. The results highlight the ability of the model to detect even sophisticated fake profiles that mimic genuine user behavior. Additionally, the system is scalable and suitable for large-scale real-world applications, particularly in rapidly growing digital environments like India. The

integration of the model with a web-based interface further enhances its practical usability for real-time detection. Overall, this work provides a robust, intelligent, and efficient solution for improving cybersecurity in social networks and mitigating the risks posed by fake accounts and botnets.

RE.FERENCES

[1] T. N. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," *Proc. International Conference on Learning Representations (ICLR)*, 2017.

[2] W. Hamilton, Z. Ying, and J. Leskovec, "Inductive Representation Learning on Large Graphs," *Advances in Neural Information Processing Systems*, vol. 30, 2017.

[3] P. Veličković et al., "Graph Attention Networks," *Proc. International Conference on Learning Representations (ICLR)*, 2018.

[4] S. Kumar, F. Spezzano, V. Subrahmanian, and C. Faloutsos, "Edge Weight Prediction in Weighted Signed Networks," *IEEE International Conference on Data Mining (ICDM)*, 2016.

[5] J. Leskovec, D. Huttenlocher, and J. Kleinberg, "Predicting Positive and Negative Links in Online Social Networks," *Proc. 19th International World Wide Web Conference (WWW)*, 2010.

[6] X. He et al., "Neural Collaborative Filtering," *Proc. International World Wide Web Conference (WWW)*, 2017.

[7] A. Grover and J. Leskovec, "node2vec: Scalable Feature Learning for Networks," *Proc. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016.

[8] B. Perozzi, R. Al-Rfou, and S. Skiena, "DeepWalk: Online Learning of Social Representations," *Proc. ACM SIGKDD*, 2014.

[9] L. Akoglu, H. Tong, and D. Koutra, "Graph-Based Anomaly Detection and Description: A Survey," *Data Mining and Knowledge Discovery*, vol. 29, no. 3, pp. 626–688, 2015.

[10] S. Cao, W. Lu, and Q. Xu, "Deep Neural Networks for Learning Graph Representations," *Proc. AAAI Conference on Artificial Intelligence*, 2016.