Question 1: Describe two applications of social network analysis (Lecture 4-1)

Answer:

Application 1: Social Media Analytics to Identify and Counter Islamist Extremism

Addressing violent extremism is a critical worldwide concern, particularly in the digital realm. Extremist factions, notably those of violent Islamist nature, exploit platforms like Twitter to disseminate radical propaganda and target susceptible individuals for recruitment. Despite recognizing the potential of big data analytics in countering extremism, there's a notable absence of a structured comprehension of the evolving landscape of online extremist narratives. The project's primary objective is to construct an online mechanism designed to detect and counteract narratives promoting violent extremism on platforms like Twitter. This initiative leverages the capabilities of big data analytics, semantic web technologies, Natural Language Processing (NLP), and crowdsourcing to fulfil four key objectives: establish an ontological model for the identification and quantification of extremist narratives, recognize the themes utilized to recruit young individuals online, evaluate the impact of propagated narratives, and incorporate an extremism ontology to guide the system's operations. The project is meticulous in differentiating the nuanced semantics of extremist narratives and incorporates domain experts to ensure precision. It employs scoring mechanisms to gauge the severity of extremist content and the influence of narratives within the realm of social media. A novel scoring system, SENIS, is introduced to measure the impact of narratives across various platforms. This project stands apart by employing an extremism ontology, gauging impact through an Islamic knowledge base (KB) and ExpertSourcing, and establishing connections with data from the Qur'an and Hadith.

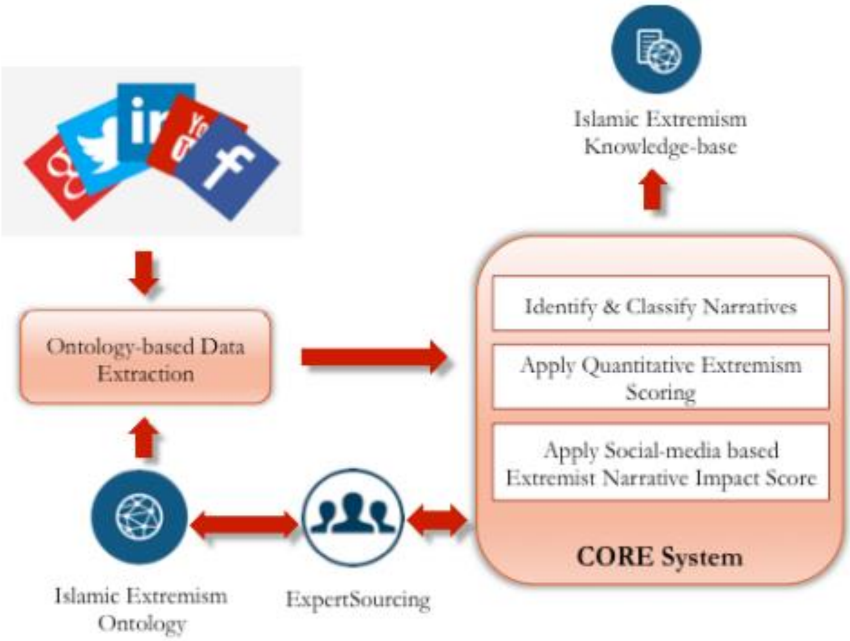

Islamic Extremism Knowledge-base
Identify & Classify Narratives
Apply Quantitative Extremism Scoring
Apply Social-media based Extremist Narrative Impact Score
CORE System
Ontology-based Data Extraction
Islamic Extremism Ontology
ExpertSourcing

Figure 1.1: Overall System Architecture

Application 2: Social Network Data Analytics for Market Segmentation in Indonesian Telecommunications Industry

The paper examines market segmentation's pivotal role in business survival within intense competition, emphasizing real-time decision-making through social media data. It zeroes in on dialogues surrounding a telecom product on Twitter, utilizing Social Network Analysis (SNA) to unveil group formations, termed "Social Network Data Analytics." The study's framework involves data collection, network construction, modularity-based group identification, and qualitative analysis of group themes, offering insights into community formation, actor involvement, size, and themes.

The modularity-based community detection's efficacy in revealing complex groupings within vast networks is highlighted. Influential actors shaping group dynamics are discussed, confirmed using centrality measurements. The paper unveils eleven dominant actors across diverse communities, differentiating service providers and customers, presenting market segmentation results. Although customer attitudes aren't definitive, a qualitative approach involving content analysis gauges perceptions of marketing components.

In conclusion, the paper underscores social network data analytics' potential in enhancing market segmentation, unearthing insights into group formations and influences. This approach expedites analysis and fortifies marketing strategies for customer satisfaction. The paper envisions expanding this approach to content analytics, bridging social network and questionnaire-based data collection.

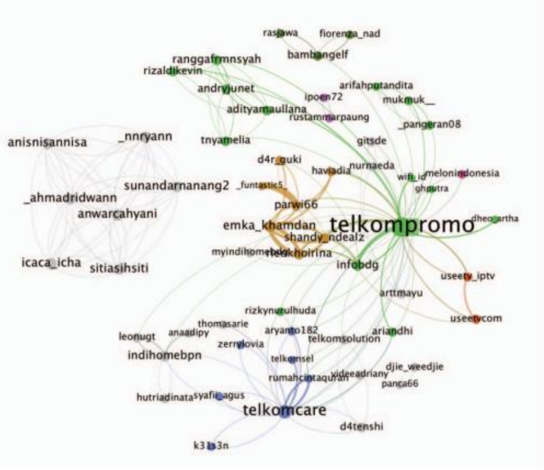


Figure 1.2: Social Network after Applying Modularity Metric

References (Including Both Figures):

Application 1: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7871051

Application 2: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8074677

Question 2: Describe the key components of the InXite Social Media System (Lecture 4-2)

Answer: Key components of the InXite social media system:

The InXite social media system is a comprehensive platform that plays a crucial role in gathering and analyzing data from diverse sources, including prominent social media platforms such as Twitter. At the core of InXite's capabilities lies its Information Engine, a sophisticated mechanism responsible for integrating data and performing various critical functions like entity resolution and ontology alignment.

To delve into the specifics, the platform's data integration process is initiated by the Information Engine, which seamlessly brings together information from multiple sources. This integrated data undergoes meticulous analysis using sophisticated data mining and machine learning techniques, all of which are facilitated by the Information Analytics Engine. The insights generated from this process are then presented to analysts for further examination and decision-making.

What sets InXite apart is its versatility, with major modules designed to cater to a wide range of applications, including Security, Marketing, and Law Enforcement. Despite the commonality among these modules, InXite takes into account the unique requirements of each application and incorporates tailored components to ensure optimal performance and relevance.

A notable feature of InXite's approach is its adaptability and flexibility. The platform adheres to a plug-and-play philosophy, granting analysts the freedom to introduce components that align with their preferences and specific tasks. This modular approach empowers users to customize the system to their advantage, enhancing efficiency and effectiveness in various scenarios.

One of InXite's groundbreaking contributions is the implementation of its proprietary algorithm, Tweethood. This algorithm, patented by InXite, predicts user attributes by leveraging the attributes of their friends. This innovative approach aids in building a more comprehensive understanding of user profiles, enhancing accuracy in attribute prediction.

InXite's capabilities extend to the analysis of threats posed by individuals. The Person of Interest (POI) Analysis is a pivotal aspect of the platform, involving a multifaceted evaluation of attributes like demographics, psychology, content, background checks, online reputation, and social graph relationships. This holistic approach to threat assessment helps organizations better comprehend potential risks and respond accordingly.

Furthermore, InXite employs advanced techniques for psychosocial analysis. This includes strategies such as micro-level location mining, which accurately pinpoints specific locations mentioned in communications, and sentiment mining, which gauges user sentiments towards specific keywords or topics. These techniques offer a deeper understanding of user behavior, helping organizations gauge sentiments and reactions more effectively.

Finally, InXite excels in threat detection and prediction. By identifying and flagging individuals who use specific keywords, the platform narrows down a pool of potential threats. The subsequent classification and grouping of flagged content are pivotal in reducing false positives and refining the prediction process. This multi-staged approach ensures that threats are accurately identified and assessed, thereby contributing to enhanced security measures.

In summary, the InXite social media system is a robust and versatile platform that amalgamates data from diverse sources, harnesses the power of advanced analytics, and provides a holistic approach to threat detection and prediction. Its modular architecture, innovative algorithms, and tailored modules make it an indispensable tool in various domains, ultimately fostering improved decision-making and risk management.

References:

[1]CS6301 Lecture #4-2 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 3: Describe sentiment analysis for social media (Lecture 4-3)

Answer: Social media holds abundant user-generated content reflecting sentiments toward various subjects. Manual review is impractical due to the volume, leading to the need for sentiment analysis. Current methods offer basic sentiment categorization, lacking detail. This study presents a novel social media analytics engine utilizing adaptive fuzzy similarity-based classification. It categorizes messages into sentiment classes and identifies emotions. Integrated into a comprehensive analysis framework, it provides a descriptive and predictive dashboard. The method is ready for user licensing.

Introduction: Social media (Twitter, Facebook, Weibo) is crucial for expressing opinions on products, services, policies, aiding sentiment analysis. Applications include aiding choices, business improvements, and political insights. Despite existing tools like Stanford NLP, Facebook Insights, TweetStats, this paper introduces a novel method. It identifies emotions (anger, sadness, happiness, excitement) based on industry patents. The paper reviews tech, introduces sentiment analysis, evaluates real data, and concludes the study.

Existing Technologies: Sentiment analysis methods fall into two categories: learning-based and lexical-based. Learning-based methods use labelled training data to predict sentiments, requiring large datasets and being contextually limited. Lexical-based methods identify sentiment indicators in text, offering wider applicability but lacking detailed emotional insights. Current lexicon-based methods face challenges in creating universal dictionaries and fine-grained emotion identification.

Various emotion research models have evolved, such as Shaver's prototypes, Ortony and Turner's hierarchy, Ekman's distinct emotions, and Plutchik's wheel of emotions. While these models contribute to emotion understanding, integrating them into sentiment analysis for advanced sensing remains rare.

This paper leverages emotion research to develop fine-grained sentiment analysis, addressing limitations in existing methods. A real-world case study demonstrates the effectiveness of public sentiments in enhancing social sensing and policy management. The insights gained aid decision-makers in refining strategies and improving products, services, and policies.

Proposed Technique: Sentiment analysis aims to detect user attitudes and emotions regarding specific topics or domains. The proposed method utilizes techniques like linguistic inquiry, ANEW approach, fuzzy logic, and emotion theories. It addresses real-world dataset challenges through a social adaptive fuzzy rule inference technique with linguistic processors. Multi-source lexicon integration is employed for sentiment and emotion analysis. An advanced linguistic processing unit with sub-modules enhances accuracy. Domain knowledge is obtained through domain lexicon knowledge extraction algorithm. The method is integrated into a social media analysis system with modules like data collection, noise filtering, sentiment & emotion analysis, predictive analysis, and results viewing. The predictive analyzer forecasts outcomes based on sentiment and emotion analysis results, aiding business activities such as forecasting and monitoring.

A real-world case study through social media analysis: While grasping the overall public reactions through sentiment valence is useful, comprehending emotions is even more crucial, especially negative ones demanding attention from decision-makers and crisis managers. As depicted in Figure 3, the ultimate result of text analysis encompasses sentiment categories and nuanced emotions. Figure 3(a) depicts sentiments, while Figure 3(b) illustrates fine-grained emotions produced by the system.

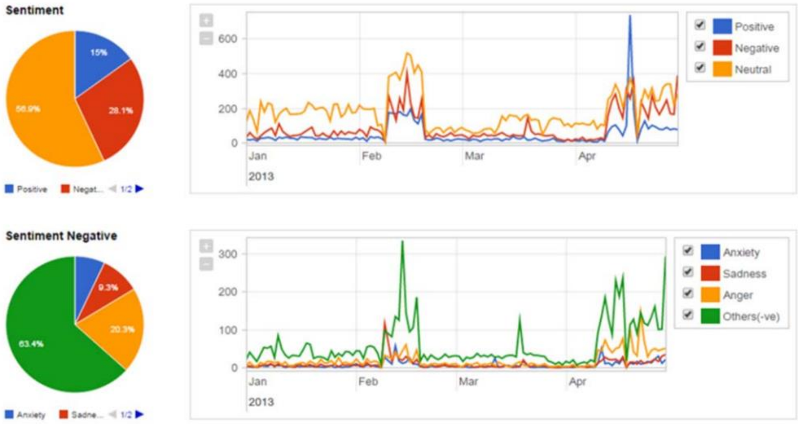
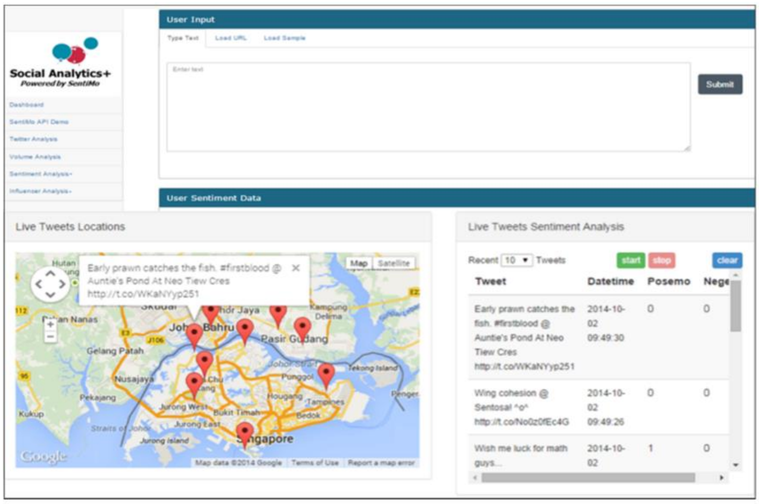


Figure 3.1(a): Sentiments depicting chart taken from [1]

Figure 3.1(b): Fine grained emotions taken from [1]

To test the proposed method in real-time, the interface for real-time data analysis is shown in Figure 3.2. Tweets serve as a test case to demonstrate real-time data collection, analysis, and visualization. Geographically tagged data is presented in a map format.



Early prawn catches the fish. #firstblood @ Auntie's Pond At Neo Tiew Cres http://t.co/WKaNYyp251

Tweet	Datetime	Posemo	Nege
Early prawn catches the fish. #firstblood @ Auntie's Pond At Neo Tiew Cres http://t.co/WKaNYyp251	2014-10-02 09:49:30	0	0
Wing cohesion @ Sentosa! ^o^ http://t.co/No0z0fEc4G	2014-10-02 09:49:26	0	0
Wish me luck for math guys...	2014-10-02	1	0

Figure 3.2: Part of the interface of the social media analytics system taken from [1]

Conclusion: The study presents an advanced approach to social media analytics that has the capacity to perform intricate sentiment and emotion analysis. This technique integrates adaptive learning, fuzzy logic, and concepts from social science to effectively categorize sentiments and emotions within textual datasets. This innovative method shows promise for diverse sectors such as healthcare, corporate, leisure, as well as both public and private domains, offering the potential to enhance customer comprehension, identify risks, and improve products and services.

References:

[1] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7821783

[2] CS6301 Lecture #4-3 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 4: Describe how terrorists/criminals may be detected in social media (Lecture 4-4)

Answer: The research introduces an advanced approach for automatically detecting extremist users on social media platforms like Twitter. It leverages as few as three groups of information—usernames, profile details, and textual content—to determine whether a given username belongs to an extremist user. The study first reveals that extremists tend to adopt usernames similar to those of like-minded individuals. The proposed detection framework utilizes features indicative of online extremism, analyzing Twitter handle patterns, profile information, and content. Various supervised and semi-supervised approaches are employed, including SVM and char-LSTM. Results on a real-world ISIS-related dataset demonstrate the effectiveness of the features in identifying online extremist users. Notably, SVM achieves a high precision of 0.96, while char-LSTM and LabelSpreading with RBF kernel yield an equal and highest F1-score of 0.76. Char-LSTM achieves a precision of 0.77 and a recall of 0.76, indicating its potential in minimizing false negatives through its memory module.

Data Preparation: The Twitter dataset comprises approximately 1.6 million tweets, posted using 25 hashtags linked to extremism like #AbuBakralBaghdadi, #ISIL, #ISIS, #Daesh, and #IslamicState. Positive labels indicating extremism were formed from 150 suspended ISIS-related Twitter handles reported to @TwitterSafety by regular users. To ensure balance, 150 random handles of normal users were collected as negative labels. Following guidance from existing literature, 13 features were grouped into three categories to identify potential extremists effectively. This resulted in 300,000 tweets with high extremism relevance, and from this pool, 3,000 handles were randomly selected.

Method: The provided feature groups identifies potential extremists and formulates key research questions. The features are categorized as follows:

Features related to Twitter handles: This category encompasses three attributes tied to the handle – its length, the count of unique characters, and its complexity. Complexity is approximated using Entropy.

Features related to user profiles: This group includes seven aspects linked to the user's profile, such as counts of followers, friends, and tweets, the presence of a profile description and location, verification status, and geo-enabled status.

Features tied to content: This section involves three features derived from tweet content – the count of URLs, hashtags, and sentiment. Sentiment is gauged by comparing negative and positive scores within the content.

For visual representation, a 2-D projection of the filtered dataset is depicted in Fig. 1, utilizing t-SNE transformation. However, standard clustering methods like K-means face challenges when labelling unlabelled instances due to limited labelled samples.

Regarding the research questions:

RQ1: Investigates whether extremists on Twitter tend to opt for similar handles.

RQ2: Explores the possibility of inferring labels (extremist vs. non-extremist) for unknown handles based on their proximity to labelled instances.

Similarity between extremist handles is gauged using the Lavenshtein ratio, indicating their inclination toward analogous handles. This trend is verified through a t-test. Additionally, the feature spaces linked to labelled and unlabelled instances are obtained, leveraging diverse handle-related attributes. These feature spaces are employed in both supervised and semi-supervised learners.

Experiments:

A. Learning Approaches:

Semi-Supervised: Various approaches including Laplacian Support Vector Machines (SVM), label spreading with Radial Basis Function (RBF) and K-nearest neighbor (KNN) kernels, and co-training with two SVMs.

Supervised: Learners such as SVM, KNN, Gaussian Naive Bayes, logistic regression, Adaboost, random forest, and Char-LSTM.

For a fair comparison, all algorithms were implemented and run in Python. For methods requiring parameter tuning, a grid search was conducted to determine optimal parameter sets. Parameters used for each learner are detailed, with the best values identified through grid search.

B. Classification Results: Tenfold cross-validation was performed on labelled data, dividing it into ten sets of equal size. One set was held for validation, while the remaining unlabelled instances were added to it. For supervised learners, the set was used solely for testing. In the semi-supervised context, both sets were used for both training and testing.

C. Feature Significance: We assess feature significance using labelled instances and the $\chi2$ feature selection measure. Results in Table III indicate that the number of unique characters in the username is the most significant feature, while the maximum number of occurrences of a character in the username is the least significant. This discrepancy illustrates that the frequency and importance of features in the labelled dataset don't necessarily align and are inversely related. Although the maximum occurrence of a character is frequent in the labelled dataset, it holds minimal importance in identifying online violent extremists.

Conclusion: This study introduced a method that utilizes minimal information from Twitter handles, profiles, and textual content to determine if a given handle might belong to an extremist user. The approach employs indicative extremism patterns initially to filter out less likely extremists, and then identifies potential extremists using username-related features. Future plans involve exploring the inclusion of additional features to potentially enhance performance. Additionally, there is a intention to integrate the feature space into a semi-supervised learner as regularization terms to further enhance classification performance in identifying online violent extremists. Considering the cost of manually labelling unlabelled examples, a promising research direction involves implementing active learning to facilitate iterative supervised learning by actively querying for labels.

References:

[1] Detection of Violent Extremists in Social Media by Hamidreza Alvari, Soumajyoti Sarkar, Paulo Shakarian

[2] CS6301 Lecture #4-4 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 5: Describe aspects of Social Media Governance and Fake News Detection (Lecture 5-1)

Answer:

Major entities involved in social media governance:

Social Media Providers are platforms like Facebook, Twitter, and similar online services that facilitate user-generated content sharing and interaction within virtual communities. Organizational (Corporate) Social Media involves organizations, including government, commercial, academic, and non-profit entities, using social media to engage audiences, promote activities, and enhance public presence.

Social Media Users actively engage with platforms for personal or professional reasons. They create profiles, share content, interact, and participate in discussions. Users, diverse in demographics and interests, contribute to the dynamic nature of social media environments.

Various aspects of social media governance and fake news detection:

1. Security Management, Administration and Governance:

The text delves into the realm of information security and its management, primarily concerned with safeguarding against risks such as information and asset loss, misuse, and damage. It underscores the significance of information security governance in harmonizing strategies with business goals and adhering to regulatory requirements. The text poses queries about the influence of social media on information security, particularly within established frameworks like BS7799/ISO 17799, ITIL, and COBIT. It underscores the imperative of amalgamating information security measures with considerations related to social media, guaranteeing alignment with business strategies, endorsement from senior management, role delineation, communication channels, legal conformity, policy formulation, guidelines, rationale for investments, and the overarching information security program.

2. Policies, Standards, Guidelines, Procedures:

This passage introduces the structure of formalized security documents, beginning with policies at the top level, giving a general perspective on asset protection. Standards offer more specific steps, guidelines provide recommendations, and procedures offer detailed instructions. The text also poses an inquiry about identifying appropriate policies, standards, guidelines, and procedures for social media systems.

3. Risk Management and Analysis:

This passage introduces essential notions concerning risk management: Risk pertains to the possibility of harm to an asset, vulnerability signifies a weakness that may be exploited, and a threat represents a potential source of harm. The interplay between threats and vulnerabilities gives rise to risk, leading to impact when actual harm occurs.

Residual risk persists even after risk management endeavors. The text subsequently poses queries about risks within social media systems and identifies those accountable for performing risk analysis.

4. Roles and Responsibilities:

Social Media Companies, such as Facebook and Twitter, formulate policies and governance decisions for their platforms, covering content guidelines, privacy settings, and user behavior rules. These decisions are made by internal teams and leadership, often guided by legal and ethical considerations. Proper governance entails striking a balance between free expression and a safe online environment.

Within Organizations, roles like Chief Social Media Officer (CSMO) oversee social media strategy, policy formulation, and alignment with goals. Key stakeholders include communications, legal, IT departments, and senior management. Well-defined roles ensure brand reputation on social media.

Social Media Users have freedom to post content, but within platform terms and guidelines. Balancing free speech with curbing offensive or false content is intricate. Platforms develop moderation policies to foster diversity while preventing hate speech and misinformation. Achieving this balance involves automated systems, human moderation, and adapting to cultural and societal norms.

The governance of social media involves collaboration among platforms, organizations, and users. It navigates between open expression and safety, evolving with technology and society.

5. Best Practices:

Best practices often involve job rotation and job sharing within organizations to enhance skills and collaboration. Applying these concepts to social media, companies could use these strategies to promote well-rounded skill development among their social media teams. Similarly, organizations can benefit from such practices in their social media departments. However, caution is needed when considering high-level roles like the Chief Social Media Officer, as frequent changes may disrupt strategic planning. Overall, these practices can be valuable, but their application should be thoughtful and context-specific.

6. Information Classification:

Classifying information according to its value and sensitivity is vital for effective security measures. In the context of social media, information classification is complex due to varying privacy settings. While some content is naturally public, users have control over their posts' visibility through platform settings. Determining what's public or private involves both user decisions and platform features, emphasizing the importance of understanding settings for maintaining desired privacy levels.

7. False/Fake Information:

Social media platforms combat the spread of fake, false, disinformation, and misinformation through content moderation, fact-checking, user reporting, algorithm adjustments, warning labels, educational initiatives, and collaboration with experts. Transparency, user empowerment, and responsible governance are crucial for effectively addressing these challenges.

References:

[1] CS6301 Lecture #5-1 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 6: Describe how data mining /machine learning may be used for fake news detection in social media (Lecture 5-2)
Answer:

Introduction: With the rise of social media as a news source, fake news is a growing concern. Social platforms facilitate quick news sharing, but also breed deliberate misinformation. This disrupts genuine news, alters beliefs, and skews responses. Detecting fake news here is complex due to varied content, deceptive intent, and reliance on non-textual cues. The article outlines challenges, notes the absence of consensus on fake news definition, reviews detection methods, and emphasizes research gaps. The survey outlines fake news features, detection methods, ongoing issues, and potential research directions.

Definitions of Fake News:
"Fake news is a news article that is intentionally and verifiably false."

Problem Definition:
This introduces news article components like publishers and content, and social news engagements that involve users spreading news. Fake news detection is formally defined as a binary classification task: predicting if an article is fake or not based on social news engagements. The task employs a prediction function F(a) that assigns 1 to fake news and 0 to real news, reflecting its link to media distortion bias. A general data mining approach is proposed, with feature extraction and model construction phases to differentiate fake news and real news using machine learning models and feature representations.

Feature Extraction:
In traditional news media, fake news detection relies on content, while on social media, extra context aids detection. We detail how to extract features from content and social context.

1. Content Features: News content includes source, headline, text, visuals. These form linguistic and visual features to spot fake news. Linguistic features identify manipulative language, while visual features analyze visual content.
2. Social Context Features: Apart from content, user interactions offer valuable insight. User-based features consider profiles, individual/group levels. Posts-based features analyze opinions, topics, credibility in posts. Network-based features study user networks, like stance, co-occurrence, friendship, and diffusion networks.

Model Construction:
Model construction be categorized into two main types: News Content Models and Social Context Models.

1. News Content Models: These models primarily rely on the characteristics of news content and factual sources. Knowledge-based approaches involve using external

sources to fact-check claims. Within this category, there are expert-oriented, crowdsourcing-oriented, and computational-oriented fact-checking methods.

Style-based methods aim to identify fake news by examining writing styles. Deception-oriented strategies focus on spotting deceitful statements through linguistic patterns. Objectivity-oriented techniques aim to uncover signs of reduced objectivity, such as hyperpartisan styles and yellow journalism.

2. Social Context Models: These models expand on the analysis of news content by incorporating social context. Stance-based models utilize user perspectives expressed in posts to infer the authenticity of news. These perspectives can be explicit or inferred from posts. Propagation-based models predict news credibility by considering relationships between social media posts. This can involve constructing credibility networks with either homogeneous or heterogeneous entities.

   Incorporating social engagements enhances the accuracy of fake news detection. Stance-based models concentrate on user viewpoints, while propagation-based models scrutinize credibility networks among posts and events.

Evaluation Metrics:

In this section, we delve into evaluating the performance of algorithms for detecting fake news, concentrating on the datasets available and the metrics used for assessment.

Datasets: Gathering online news data poses challenges due to the need for experts to confirm authenticity, involving annotators with specialized knowledge. Datasets with annotations can be obtained through expert journalists, fact-checking websites, industry detectors, and crowdsourced workers. Some publicly accessible datasets include BuzzFeedNews, LIAR, BS Detector, and CREDBANK. However, these datasets have constraints, like incomplete content, skewed labels, or dependence on specific tools for annotation.

To address these limitations, an ongoing project is crafting a dataset named FakeNewsNet for detecting fake news on social media. This dataset encompasses comprehensive features and dependable ground truth labels.

Evaluation Metrics: To gauge algorithm performance in fake news detection, diverse evaluation metrics are utilized. The problem is treated as a classification task that forecasts whether a news article is genuine or fake. Standard metrics encompass:

Precision: Proportion of predicted fake news correctly classified as fake.

Recall: Proportion of actual fake news articles accurately predicted as fake.

F1 Score: Harmonic mean of precision and recall.

Accuracy: Fraction of news articles correctly classified.

Precision and recall are pivotal for distinguishing fake news and its sensitivity, correspondingly. The ROC curve illustrates the trade-off between False Positive Rate (FPR) and True Positive Rate (TPR). The Area Under the Curve (AUC) quantifies a classifier's capability to rank fake news higher than true news. AUC proves particularly valuable for unbalanced classification issues, as observed in fake news detection.

References:

[1] Misinformation in Social Media: Definition, Manipulation, and Detection
[2] CS6301 Lecture #5-2 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 7: Describe how data mining /machine learning may be used for fake news detection in social media (Lecture 5-3)

Answer: Social media's role in news consumption is a double-edged sword. Its accessibility, speed, and affordability encourage news consumption, but it also fosters the rapid spread of "fake news" - news with deliberately false information. Detecting fake news on social media is vital due to its potential harm. This emerging research area faces unique challenges, distinct from traditional media. Fake news often requires auxiliary information like user engagement to detect, given its intentional misleading nature. However, utilizing such data is complex due to its volume, incompleteness, and noise. To address these challenges, the authors conducted a survey, reviewing fake news detection in social media comprehensively. They cover characterizations of fake news from psychological and social perspectives, data mining algorithms, evaluation metrics, datasets, related research areas, and future directions.

Introduction:

As people increasingly rely on social media for news, the spread of fake news has become a concern. Despite its advantages, including speed and accessibility, social media is plagued by low-quality news containing false information. Fake news, intentionally misleading content, can disrupt the authenticity of news and sway beliefs. Detecting it on social media is challenging due to its deliberate deception and the noise in user-generated data. The authors highlight the need for clear definitions and overview methods while emphasizing ongoing research for more effective detection and mitigation.

Using data mining /machine learning for fake news detection in social media:

The authors' examination of fake news detection within the context of social media underscores the significant role that data mining and machine learning can play in addressing the proliferation of misinformation. They delve into a comprehensive framework that harnesses these technologies to tackle the intricate challenge of differentiating between genuine and fabricated news.

Data mining assumes a crucial function by extracting valuable insights from the massive reservoir of data generated through users' interactions on social media platforms. Machine learning algorithms then assimilate these insights to construct models capable of effectively discerning authentic news from deceptive content. The efficacy of these models hinges on the quality and relevance of the features they incorporate.

The analysis of news content features—ranging from source information and headlines to textual elements and even visual content like images and videos—employs advanced techniques to capture telltale signs of fake news. Language patterns and writing styles, exploited by those behind fake news to evoke emotional reactions, are subjected to quantification and analysis through linguistic-based features. These features encompass metrics like word usage frequency, sentence structures, and syntactic components.

Moreover, the authors emphasize the integration of supplementary data derived from the social context. They recognize that the sharing, commenting, and discussions related to news on social media platforms provide insightful cues about its authenticity. Characteristics linked to users' engagement patterns, including individual profiles, group-level behaviors, and the temporal evolution of interactions, collectively contribute to developing a more holistic understanding of how news propagates.

Machine learning techniques are harnessed across two pivotal phases: the extraction of features and the construction of models. The authors underscore the necessity of crafting meaningful feature representations that encapsulate the subtleties of fake news. These features, whether originating from content specifics or the social context, serve as the input to machine learning models. These models can range from conventional methodologies like classification algorithms to more sophisticated approaches such as deep learning.

Ultimately, the authors' analysis underscores the formidable potential of data mining and machine learning in countering fake news within the intricate domain of social media. By amalgamating insights from both content and user engagement, these techniques provide a promising avenue for effectively identifying and mitigating the dissemination of misleading information. The outcome is a more enlightened and resilient online community.

References:

[1] Fake News Detection on Social Media: A Data Mining Perspective by Kai Shu, Amy Silva, Suhang Wang, Jiliang Tang, and Huan Liu

[2] CS6301 Lecture #5-3 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 8: Describe aspects of Cyber Bullying in Social Media (Lecture 5-4)

Answer:

Increased social media usage has heightened the threat of cyberbullying among youth. Previous research mainly focused on pinpointing cyberbullying in individual texts, leaving a gap in understanding its occurrence throughout complete social media sessions. These sessions include initial posts, multimedia, comment sequences, user interactions, location details, and more social content. Examining cyberbullying within sessions enables researchers to delve into its repetitive nature and power imbalances. The article emphasizes the need to explore session-based cyberbullying detection, outlines key challenges, and suggests future research directions.

Introduction:

Cyberbullying is on the rise, affecting around 36.5% of people. Although its definition varies, it involves deliberate electronic aggression towards vulnerable individuals, characterized by power imbalances and repetition. Current detection methods focus on text analysis using Natural Language Processing (NLP), yet they struggle to capture power dynamics and repetition. Adapting these methods to social media's complexities—real-time, spatial, emotional—poses challenges. To overcome these, a session-based approach, considering posts, media, comments, and interactions, offers a broader perspective. This strategy reveals evolving power dynamics, recurring patterns, and hierarchical structures. Embracing session-based cyberbullying detection expands beyond text analysis, opening doors for comprehensive research and prevention.

Definition: "The author defines session-based cyberbullying detection as the identification of cyberbullying behavior within a social media session by leveraging multiple media objects including textual features, user interactions, spatial location, temporal information, visual cues, social network, and other social attributes, e.g., users' profile information."

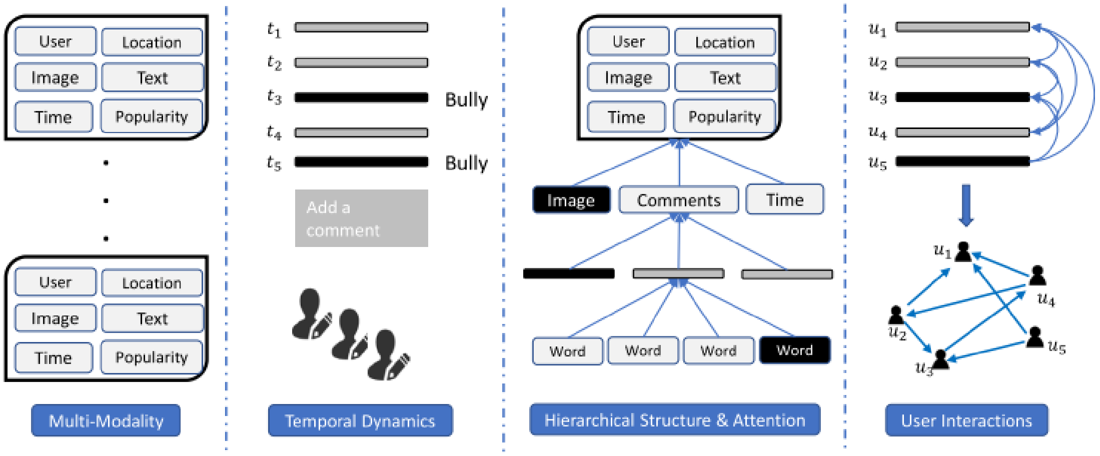


Figure 8.1:

Session-based cyberbullying detection introduces four distinct characteristics, as depicted in Figure 8.1. Firstly, it acknowledges multimodality, recognizing the diverse modes of interaction on social media, such as images, comments, and captions, which provide opportunities for bullies to target victims. Secondly, it considers temporal dynamics as social media sessions evolve through increasing user comments, enabling the examination of the recurring nature of cyberbullying across the session's history. Thirdly, it incorporates the hierarchical structure and attention inherent in social media sessions, enhancing the representation of sessions and allowing for an exploration of the significance of different media objects. Lastly, it uncovers intense user interactions that unveil indirect cyberbullying occurring within interactions, shedding light on roles like bullies in evolving conversations.

Challenges of Session-based Cyberbullying Detection:

Detecting cyberbullying within complex social media sessions introduces distinct challenges and avenues for advancement compared to traditional approaches. These challenges encompass the unique traits of social media sessions and factors related to data collection, such as safeguarding privacy and labeling data.

Multimodal Context: Social media sessions encompass diverse modalities like text, images, and locations. However, incorporating this multimodal context is intricate due to the extensive range of feature values and the necessity to capture connections between different modalities. This complexity can lead to sparsity issues as each modality's training data is limited. Addressing structural links among sessions and modalities is pivotal.

Temporal Dynamics: Cyberbullying manifests as a continuous temporal phenomenon rather than isolated events. To capture the dynamic nature of social media sessions, temporal analysis is crucial. Techniques such as point processes, multitask learning, and burst analysis have been utilized to model temporal characteristics effectively.

Hierarchical Structure and Attention: Social media sessions comprise various media components like comments, images, and timestamps. Effectively modeling this hierarchical structure while enabling adaptable attention to different elements enhances session representation and understanding of media object significance.

Modeling User Interactions: Conventional cyberbullying detection often neglects the sequence of interactions, focusing solely on individual posts or users. Analyzing evolving conversations and constructing interaction networks enables the identification of unique user roles and patterns.

Privacy Protection: Balancing cyberbullying detection with user privacy is crucial. Users may want to limit data access due to privacy concerns, and adhering to privacy regulations presents complexity. Striking a balance between privacy preferences, data utility, and model performance is a multifaceted challenge.

Data Labeling: The process of labeling data is labor-intensive and complicated by the array of social media session components. Incorporating information from diverse modalities is imperative during the labeling process. Imbalanced datasets with limited instances of cyberbullying can impact model efficacy, necessitating careful handling of training and testing data distributions.

References:

[1] Session-based Cyberbullying Detection: Problems and Challenges

[2]CS6301 Lecture #5-4 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 9: Describe how Data Science and Cyber Security may be integrated to provide security and privacy for Internet of Transportation Networks (Lecture 6-1)
Answer:

Big Data Management, Security and Privacy:
Technological progress has made it feasible to process and analyze vast amounts of data for security purposes. These tasks encompass user authentication, access control, anomaly detection, monitoring, and safeguarding against insider threats. Through the analysis and integration of web-derived data, connections between individuals can be identified, offering potential benefits for homeland security and disease tracking. However, even if data is de-identified, linking it to other sources can result in identifying individuals. Security tasks like authentication require sensitive user information, which if mishandled can lead to privacy breaches. Future focuses include securing data through access control models, privacy-enhancing techniques, big data analytics in cybersecurity, and ensuring the security of machine learning processes.
Privacy Aware Quantified Self:
The use of mobile devices such as smartphones have become highly popular, and the Quantified Self (QS) movement involves analyzing personal data from wearables and apps to assist users in enhancing their health and lifestyle. This data is often shared with other service providers through cloud services, providing advantages such as health insights. Nevertheless, this sharing frequently happens without user awareness, creating a significant risk of personal data misuse. For instance, health data collected might be exploited by insurance companies to reject coverage. The combination of financial, health, and social media data could result in serious repercussions. To address these challenges, there is a pressing need for privacy protection tools and techniques in QS applications.
Policy Aware Data Collection, Storage, Access, Analytics, Learning and Sharing:
As data accumulation grows, the device's storage capacity becomes insufficient. A proposed solution involves encrypted cloud storage for less frequently accessed or older data. Local apps will adhere to access control policies, gaining access to specific data. Apps can retrieve encrypted cloud-stored data using a query interface. Data relevance may lead to storing monthly averages instead of fine-grained data, or data deletion for privacy reasons. Data sharing and analytics will be facilitated by cloud services, accommodating different scenarios with modified or encrypted data transmission as required.
Data Science for Cyber Security Applications: Big Data Stream Classification:
Uses past data to build classification model: This refers to the process of utilizing historical data to develop a predictive model. In the context of classification, the model learns patterns and relationships from past data where instances are already labeled with specific classes. For example, in email spam detection, the model learns from past

emails labeled as "spam" or "not spam" to distinguish between the two categories based on various features.

Predicts the labels of future instances using the model: Once the classification model is trained on past data, it can be used to predict the labels or categories of new, unseen instances. These new instances may not have known labels initially. The model's ability to predict the correct class for these instances based on the patterns it learned during training is a crucial aspect of its functionality.

Helps decision making: Classification models play a significant role in aiding decision-making processes. By predicting the class of a new instance, the model provides valuable insights that can guide decisions. For instance, in a medical setting, a classification model trained on patient data can assist doctors in diagnosing diseases or recommending appropriate treatments based on the predicted medical condition.

Big Data Streams:

Continuous flow of data: Big data streams refer to the continuous and uninterrupted flow of data. Unlike traditional batch processing where data is processed in predefined chunks, data streams are dynamic and ongoing, often generated by various sources simultaneously.

Common in our connected digital world: In our interconnected digital environment, data streams are prevalent. Internet of Things (IoT) devices, social media interactions, online transactions, and sensor networks constantly generate data streams that provide real-time insights.

Massive amounts of data: Big data streams can involve massive volumes of data being generated at high speeds. These data streams need to be processed, analyzed, and acted upon quickly to extract meaningful information and respond in a timely manner.

References:

[1]CS6301 Lecture #6-1 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 10: Describe how knowledge graphs may be used to represent attack data and subsequently reason about the data to help cyber security analysis (Lecture 6-2)

Answer:

Cyber threats are evolving and target individuals and organizations. Security Analysts in Security Operations Centers (SoC) require up-to-date threat intelligence. A pipeline can gather, extract, and structure web-based threat data for Security Information and Event Management (SIEM) systems. These systems use knowledge graphs (KGs) to store and retrieve threat information. Semantic triple generation, involving entities and relationships, is crucial for KGs. The proposed RelExt system enhances cyber threat representation by predicting relationships between cybersecurity entities through neural networks. This aids Analyst Augmentation Systems for SoCs, improving overall cybersecurity. The system employs contextual vector representations of identified entities. The paper covers related work, ontology creation, introduces RelExt, evaluation metrics, and concludes.

Cyber Security Knowledge Graph:

Cybersecurity Knowledge Graphs (CKGs) comprise a schema for structure definition and semantic triples for entity relationships. Constructing a CKG begins with outlining the schema, specifying entity classes and potential relationships. 'RelExt', the proposed system, employs deep learning to predict and extract relationships from cybersecurity entities in text, enhancing the CKG's accuracy and usefulness.

The Unified Cybersecurity Ontology (UCO) serves as a foundational framework for CKG development. UCO 2.0 expands upon this, incorporating concepts from STIX 2.0, a cybersecurity threat sharing standard. UCO 2.0 defines classes like Software, Malware, Indicator, etc., and establishes relationships such as 'hasProduct', 'hasVulnerability', and more.

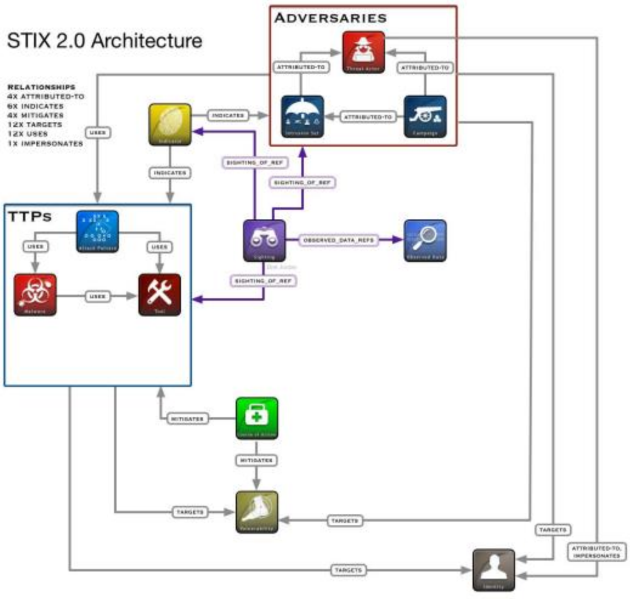


Figure 10.1: Architecture

The key contribution of 'RelExt' lies in its capability to enhance CKGs by validating and suggesting missing relationships. Incorrect or absent relationships in CKGs can lead to inaccuracies. 'RelExt' addresses this by automatically proposing relationship values based on text context.

The integration of 'RelExt' and UCO 2.0 promises a refined representation of cybersecurity information in knowledge graphs. This enhancement promotes more effective cybersecurity analysis, decision-making, and threat detection.

RelExt: System Architecture

This section presents the architecture of the RelExt system, designed to extract relationships between pairs of named entities within cybersecurity text. RelExt takes entity pairs as input and generates an entity relationship set as output. To identify cybersecurity entities, a Named Entity Recognizer (NER) is utilized, borrowed from the CyberTwitter system. The NER categorizes entities using a key-value structure, where the key signifies a cybersecurity entity and the value corresponds to a UCO 2.0 class.

Further processing of RelExt's input aligns with the cybersecurity knowledge graph's schema to ensure coherence. Inconsistent or irrelevant entity pairs are filtered out, with proximity optimization focusing on entity pairs within a designated word window of 35 words.

The system employs a feed-forward neural network (FFNN) classifier named RelExt to forecast relationships between named entities. These entities are represented as vector embeddings generated using the Word2Vec model, trained on cybersecurity text data. Comprising input, output, and three hidden layers, the FFNN model employs the sigmoid function for activation. The FFNN's predictions contribute to enriching cybersecurity knowledge graphs.

The output from RelExt, comprising relationship sets for entity pairs, is then integrated into the cybersecurity knowledge graph. A section of the text illustrates a subset of this knowledge graph, revealing relationships, classes, and entities linked to malware attacks. This knowledge graph facilitates capturing intricate relationships, dependencies, and vulnerabilities among entities, aiding in the analysis of cybersecurity threats and uncovering insights from similarities between different attacks.

References:

[1] RelExt: Relation Extraction using Deep Learning approaches for Cybersecurity Knowledge Graph Improvement

[2]CS6301 Lecture #6-2 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas

Question 11: Describe aspects of Vehicular Social Networks (Lecture 6-3)

Answer:

Vehicular Social Networks (VSNs) merge VANETs and MSNs, opening new research paths for content sharing, data dissemination, and delivery. SNA analyzes entity relationships for applications. VSNs involve interactions among commuters, creating virtual vehicle communities. This paper explores VSN potential, communication, and innovative systems using social behaviors and mobility. It reviews socially-aware VSN applications, covering data dissemination and mobility modeling. The authors discuss recommendation systems, path planning, crowdsourcing, and cloud computing, and outline future research directions.

Vehicular Social Networks:

Commuters who follow similar routines and social behaviors while facing comparable traffic conditions form virtual communities on roads. These communities exhibit traits from social networks, such as shared interests and predictable travel patterns. However, these relationships are not as strong as those in traditional online social networks (OSNs). Vehicular Social Networking (VSN) aims to integrate the social behaviors of commuters in vehicular environments. VSNs leverage social properties, shared interests, and objectives among vehicles, drivers, passengers, and pedestrians using smart devices. This concept combines elements from Vehicular Ad-Hoc Networks (VANETs) and social networks, utilizing VANETs for communication infrastructure and social networks for social knowledge.

Architecture:

Vehicular Social Networks (VSNs) consist of participants using mobile devices and vehicular network infrastructure. Beyond just drivers, passengers, pedestrians, and On-Board Units (OBUs) also engage in communication within VSNs. Smart devices in vehicles and on individuals can detect proximity and share content, allowing users to be publishers, subscribers, or both. Communication in VSNs falls into three categories: humans-to-humans, humans-to-machines, and machines-to-machines. The physical architecture of VSNs relies on vehicular network infrastructure and software platforms. Applications can be designed for centralized, distributed, or hybrid VSNs, which are categorized based on their communication architecture.

Centralized VSNs involve communication with centralized service providers, acting as bridges between users/platforms. In distributed VSNs, vehicles communicate independently without a centralized server, collaborating in an ad-hoc manner using Vehicle-to-Vehicle (V2V) contact. Hybrid VSNs combine direct V2V and Vehicle-to-Infrastructure (V2I) communication, enabling diverse applications like traffic efficiency improvement and infotainment. Commuters may also use cellular data if roadside infrastructure is unavailable.

Application:

Vehicular Social Networks (VSNs) provide applications that fall into four distinct categories: safety, convenience, comfort, and entertainment. Safety applications are geared towards enhancing road safety, while convenience applications aim to optimize traffic flow and reduce travel time. Comfort applications are designed to elevate the commuter experience by offering services such as toll payments and parking assistance. Meanwhile, entertainment applications enable the sharing of music, videos, and games for enjoyment while driving.

Socially Aware Applications in VSNs:

Within the emerging landscape of Vehicular Social Networks (VSNs), drivers and passengers are enabled to establish connections and engage in sharing activities within virtual communities present on roads. For instance, individuals journeying towards a particular city may exchange their driving encounters and details pertaining to lodgings and dining establishments. The credibility of recommendations holds significant value. Vehicular units establish social clusters using Vehicle-to-Vehicle (V2V) communication, facilitating content sharing grounded in shared interests and affiliations. During peak traffic hours, vehicles can spontaneously form virtual communities for discussions spanning weather updates, news, traffic conditions, and entertainment. Social attributes play a pivotal role in enabling socially-aware V2V communication, amplifying interactions among individuals with similar destination trajectories. Prominent online platforms such as Facebook and Twitter serve as inspirations for these socially-conscious applications. Notably, even in the absence of centralized infrastructure, drivers and passengers retain the capability to communicate directly, disseminating information based on their social alignments within these vehicular communities.

Data Dissemination in VSNs:

Vehicular Social Networks (VSNs) facilitate interactions and information sharing among commuters, functioning within a dynamic and opportunistic distributed framework. Challenges within VSNs encompass comprehending social dynamics, coping with dynamic network topology, and addressing intermittent connectivity. Social Network Analysis (SNA) is employed to optimize data dissemination, employing metrics like node degree, closeness centrality, and betweenness centrality. These metrics aid in pinpointing crucial nodes for efficient data transmission. VSN performance is contingent upon application requirements, whether focused on road safety or delay-tolerant tasks. The formation of virtual communities comprising commuters with akin mobility patterns enhances the efficacy of data delivery. Prospects for enhancement involve incorporating mobility patterns, social affinity, communication infrastructure, and user preferences across diverse VSN applications.

Vehicular Mobility in VSNs:

In Vehicular Social Networks (VSNs), the movement of vehicles is limited to roads and highways, facilitating the exchange of information for diverse applications. Mobility in this context is influenced by various factors including human behavior, traffic management, social attributes, daily routines, and user preferences. The utilization of crowdsourcing within VSNs enriches intelligent transportation, enabling users to share real-time information about parking availability, route options, restaurants, and more. These applications not only tackle traffic congestion but also provide vehicles with updates on anomalies, events, and accidents. VSN research focuses on crucial areas such as mobility modeling, recommendation systems, and route discovery/planning. Mobility models capture social dynamics and connectivity, while recommendation systems harness social interactions to offer services like identifying points of interest. Route discovery and planning combine established algorithms with human behavior considerations to optimize travel paths.

References:

[1]CS6301 Lecture #6-3 Course Material, Dr. Bhavani Thuraisingham, The University of Texas at Dallas