

An Analytical Review of Kalman Filter Models for Prediction and Security of Twitter-Derived Road Traffic Data

Ahmad Faisal Abidin

Department of Computer Science, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Terengganu, Malaysia

Nor Surayati Mohamad Usop

Department of Computer Science, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Terengganu, Malaysia

Mohd Fadzil Abdul Kadir

Department of Computer Science, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Terengganu, Malaysia

Mohamad Afendee Mohamed

Department of Computer Science, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Terengganu, Malaysia

Abstract:

The growing use of social media platforms, particularly Twitter, for real-time reporting of road traffic conditions presents new opportunities for intelligent transportation systems. However, traffic data derived from Twitter is inherently noisy, unstructured, and susceptible to misinformation, which poses significant challenges to prediction accuracy and data security. This review paper provides an analytical examination of Kalman Filter (KF)-based models for enhancing the reliability, robustness, and integrity of traffic information extracted from Twitter. The study focuses on variations of the Kalman Filter, with particular emphasis on the Extended Kalman Filter (EKF), and evaluates their effectiveness in handling uncertain, incomplete, and dynamically evolving data patterns typical of social media streams. Furthermore, the review discusses the role of KF-based prediction in supporting anomaly detection mechanisms for identifying malicious, manipulated, or bot-generated traffic reports, thereby improving data authenticity and trustworthiness. Existing studies indicate that Kalman Filtering techniques enhance traffic flow prediction accuracy, reduce noise in user-generated content, and improve model stability in rapidly changing traffic environments. Despite these advantages, several challenges remain, including scalability, semantic interpretation of textual data, and integration with cybersecurity frameworks such as sentiment analysis, machine learning-based classification, and blockchain-enabled validation. The paper concludes that Kalman Filter models hold strong potential

for securing and predicting Twitter-sourced traffic data; however, further interdisciplinary research is required to develop optimized hybrid systems that integrate natural language processing, advanced filtering techniques, and robust security frameworks.

Keywords:

Kalman Filtering, Traffic Prediction, Data Security, Social Media Analytics, Twitter Traffic Data.