International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Securing Mobile Networks: Identifying Route Hijacking in Opportunistic Scenarios

[1]Jyothika K R, [2] Varun Kumar A M

[1]*Assistant Professor, Department of MCA, BIET, Davenagere*

[2]*Student, 4th Semester MCA, Department of MCA, BIET, Davanagere*

ABSTRACT

This paper investigates the security vulnerabilities of Hybrid Routing and Prophet protocols in Opportunistic Mobile Networks (OMNs), highlighting their susceptibility to a novel threat called the CollusiveHijack attack. In this scenario, an adversary—referred to as Eve— compromises multiple nodes and intentionally falsifies Inter-Contact-Time (ICT) data to exaggerate the frequency of node encounters. By misrepresenting these metrics, Eve successfully manipulates routing decisions and intercepts network traffic. This manipulation facilitates more advanced attacks such as traffic eavesdropping, packet tampering, and exploitation of network incentives.

To counteract this threat, we introduce a detection framework based on the Kolmogorov- Smirnov two-sample statistical test. This approach examines whether the observed delay distribution of packet delivery aligns with the expected distribution derived from ICTs. We develop three detection strategies—Path Detection Technique (PDT), Hop Detection Technique (HDT), and Early Hop Detection Technique (EHDT)—each balancing between security protocol compatibility, detection effectiveness, and response time.

Our evaluation, comprising detailed trace-driven simulations and a prototype implementation, demonstrates the efficacy of these methods. Specifically, the proposed techniques achieve detection rates ranging from 80.0% to 99.4% when Eve captures over 60 packets, with low false positives (~3.6%) and rapid detection times (7–14 hours). The EHDT method, in particular, offers up to 85% faster detection compared to PDT and HDT.

Keywords: Opportunistic Mobile Networks (OMNs), CollusiveHijack attack, Inter-Contact- Time (ICT), Prophet protocol, Kolmogorov-Smirnov test, Packet delay distribution, Path Detection Technique (PDT), Hop Detection Technique (HDT), Early Hop Detection Technique (EHDT).

1. INTRODUCTION

Opportunistic Mobile Networks (OMNs) have emerged as a critical solution for communication in environments where traditional infrastructure is absent or unreliable. These networks rely on intermittent contacts between mobile nodes to forward messages, making routing decisions based on historical contact patterns, such as Inter-Contact Times

(ICTs). Protocols like Hybrid Routing and Prophet have proven effective in such settings, leveraging ICTs to estimate the probability of successful message delivery.

However, the reliance on ICT-based metrics also introduces significant vulnerabilities. In this paper, we explore a new attack model, called the *CollusiveHijack* attack, in which an adversary manipulates ICTs to mislead routing protocols. A malicious entity— Eve—strategically compromises multiple nodes and falsely advertises frequent contacts between them. By doing so, Eve can attract and hijack message flows, positioning

herself in the routing paths of legitimate nodes. Once in control, she can launch further attacks such as data modification, traffic analysis, and unauthorized incentive claiming in reward- based routing systems.

The subtle nature of the CollusiveHijack attack makes it difficult to detect using traditional security mechanisms. It does not rely on overt interference or packet dropping but rather on deception within routing metric calculations. Consequently, detecting such an attack requires a statistical approach that can highlight discrepancies between the expected and observed behavior of packet delivery.

To address this, we propose the use of the **Kolmogorov-Smirnov (KS) two-sample test** to statistically evaluate whether the observed packet delay distributions align with those predicted from ICTs. If a discrepancy is found, it indicates possible manipulation in the routing information. Building on this concept, we design three detection techniques—Path Detection Technique (PDT), Hop Detection Technique (HDT), and Early Hop Detection Technique (EHDT)—each tailored for different trade-offs in detection latency, accuracy, and protocol compatibility.

Through rigorous simulations using real- world mobility traces and a proof-of- concept implementation, we validate the effectiveness of our techniques. Our results show high detection accuracy with low false positives and short detection delays, demonstrating the practicality of our approach in enhancing the security and reliability of routing in OMNs.

II. LITERATURE REVIEW

C. Yang and R. Stoleru, A hybrid routing strategy for heterogeneous wireless networks was presented in their paper "Hybrid routing in wireless networks with diverse connectivity" (Proc. 17th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2016, pp. 71–80). In a different recent study on recruitment fraud detection, researchers suggested a novel method to more accurately detect phony job postings by using transformer-based deep learning models, BERT and RoBERTa. They combined job postings from three distinct sources to create an improved dataset after realizing the shortcomings of the benchmark datasets that were already in place. Ten excellent SMOTE (Synthetic Minority Oversampling Technique) variants were used to rectify the notable class imbalance found by exploratory data analysis (EDA). The BERT model in conjunction with SMOBD SMOTE produced the best balanced accuracy and recall.[1]

S. Datta and S. Madria, In their paper *“Efficient photo crowdsourcing with evolving POIs under delay-tolerant network environment”* (Pervasive Mobile Comput., vol. 67, 2020, Art. no. 101187),
S. Datta and S. Madria present an effective photo crowdsourcing technique intended for disaster or battlefield situations where communication infrastructure is not available. In these settings, nodes—such as soldiers, rescue personnel, or survivors— gather photos of Points of Interest (POIs) that have been located by a central server and distribute them via a store-and-forward, delay-tolerant communication model. Situational awareness is preserved even in the face of severe and disjointed circumstances thanks to this method, which allows the gradual transfer of crucial image data to the command center via opportunistic node-to-node transmission.[2]

Firechat: Google Play Store, 2022. A disaster response app called Firechat is helpful in emergency situations because it allows off-grid communication without internet or cellular networks. Because Firechat is relevant to both the general public and first responders, it was placed under Communication/Reunification in a 2022 review of 927 emergency apps from the Google Play and Apple iTunes stores. The study emphasized the need for ongoing evaluation while highlighting the increasing quantity and development of such apps.[3]

Y. Liu, examines In order to facilitate communication that is resistant to censorship and surveillance, Delay Tolerant Networks (DTNs) constructed using common smartphones. To collect data on real-world wireless connectivity, 111 users of the prototype DTN-based microblogging app 1am were placed in a college

town. Based on this data, simulations revealed that 85% of messages were delivered within a week with a median delay of 13 hours, despite only 0.2% adoption. The system demonstrated the usefulness of DTNs in constrained settings by remaining resilient even after attacks destroyed more than half of the nodes and using less than 10% of a smartphone's daily battery.[4]

E. Harkavy and M. S. Net, a reinforcement learning-based method to automatically handle buffer overflows in DTN nodes, especially in deep space communications where traditional protocols like TCP/IP don't work. When buffer capacity is almost full, their technique allows an agent to do one of three things: slow the client, request additional resources, or drop packets. The study highlights the applicability of reinforcement learning in situations where human intervention is impractical by demonstrating the viability and practicality of implementing such autonomous buffer management using present and future DTN and Deep Space Network capabilities.[5]

E. Tikhonov, D. Schneps-Schneppe, and D. Namiot, In the context of growing railway communication networks, where trains function as mobile nodes exchanging telemetry data and messages, this paper examines Delay Tolerant Network (DTN) protocols. The study compares DTN protocols in terms of buffer load and delivery delay under various network loads and mobile coverage scenarios using a real European railway line scenario. The performance of DTN protocols during the switch to faster networks, such as 5G, is also examined in the paper, emphasizing how well they preserve communication reliability in the face of sporadic connectivity.[6]

J. Wu, Y. Guo, H. Zhou, L. Shen, and L. Liu, The routing algorithm for Vehicular Delay Tolerant Networks (VDTNs), in which cars function as mobile nodes with predictable movement patterns, is presented in this paper using a Bayesian Network (BN). In contrast to conventional DTN algorithms, the suggested approach makes use of these patterns by building a BN model that combines several node attributes for a more precise prediction. A hybrid K2- Genetic Algorithm (K2-GA) is presented in order to optimize the BN structure, and the Junction Tree Algorithm (JTA) is used to speed up inference. The algorithm's effectiveness in actual VDTN scenarios is demonstrated by simulations that show increased delivery ratios with low forwarding overhead.[7]

Y. Dong, F. Zhang, In order to overcome the problem of selfish nodes that decline to forward messages because of resource limitations, this paper suggests a multi- relay selection algorithm for vehicular delay-tolerant networks (VDTNs) based on Q-learning. The algorithm prevents uncooperative nodes from being chosen as relays by giving each node a credit value determined by its historical behavior. It uses buffer optimization to lessen congestion and combines credit evaluation and Q-learning to enhance routing choices. In comparison to conventional routing techniques, simulation results demonstrate improved delivery probability, decreased message latency, and decreased network overhead.[8]

III. EXISTING SYSTEM

In the current Opportunistic Mobile Networks (OMNs), routing protocols like PRoPHET and Hybrid Routing are widely used. These protocols depend on historical encounter data, particularly Inter-Contact Times (ICTs), to make forwarding decisions. Nodes exchange their encounter probabilities and use this information to route data in the absence of end-to-end paths. These systems perform reasonably well in scenarios where all participating nodes behave honestly and share truthful encounter data.

However, these routing systems operate without security validation mechanisms, which creates a significant loophole. They assume node honesty and do not have any in-built system to verify the truthfulness of the ICT data. If a malicious node or group of nodes (as in the case of CollusiveHijack attacks) fakes encounter histories, they can manipulate routing paths to attract or divert traffic. Such manipulated routing can lead to attacks like packet hijacking, modification, traffic analysis, and blackholing.

Disadvantages of the Existing System

No validation of ICTs or encounter probabilities — leads to easy manipulation. Vulnerable to collusive behavior by multiple malicious nodes. Cannot detect subtle, statistical attacks like

CollusiveHijack.

Depends heavily on trust-based forwarding, which is unsafe in hostile environments.Lack of machine learning or adaptive behavior — does not learn from previous attack patterns. Existing security mechanisms (if any) are not suitable for intermittent connectivity scenarios. Inability to provide early warning or predictive analysis before damage occurs.

IV. PROPOSED SYSTEM

To overcome these limitations, the proposed system introduces a data-driven, machine learning-based framework to detect and prevent route hijacking attacks, particularly CollusiveHijack. In this model, users input dataset parameters such as ICTs, delays, node interactions, and path details. These values are processed using trained ML classifiers like Logistic Regression, Random Forest, SVM, and Decision Trees to predict whether the routing pattern is legitimate or under attack.

The system integrates statistical testing (Kolmogorov-Smirnov Test) to compare the observed delay patterns with the expected patterns derived from ICTs. Discrepancies between these distributions act as indicators of data falsification. Furthermore, three detection models— PDT, HDT, and EHDT—are used to identify attacks either across full routes, per-hop basis, or at early stages for rapid intervention.

A user-friendly web interface built using Flask allows real-time data entry, route monitoring, and prediction output. The entire system is lightweight, scalable, and compatible with existing OMN routing protocols.

Advantages of the Proposed System

High detection accuracy (80% to 99.4%) with minimal false positives (~3.6%). Uses machine learning models to identify patterns of malicious behavior.

Capable of early detection using EHDT (within 7–14 hours). Applies statistical analysis (KS Test) to catch falsified ICTs effectively. Provides a clear “Attack” or “Not Attack” result, improving decision- making.

Web-based interface ensures easy integration and usability. Compatible with existing OMN systems without altering their architecture. Adaptable to new data, allowing continuous learning and system improvement.

System Architecture

Fig 1. System Architecture

V. MODULE DESCRIPTION

The proposed system is designed to detect route hijacking attacks in Opportunistic Mobile Networks (OMNs) by analyzing communication patterns and packet delays using statistical and machine learning methods. To facilitate user interaction and prediction analysis, the system is divided into three main functional modules: User Registration and Login, Home Page, and the Prediction Page.

The User Registration and Login module provides the foundation for a secure and personalized experience. New users are required to create an account by entering their details such as name, email address, and password. This registration process includes input validation and secure handling of user credentials, typically by hashing passwords before storing them in the database. Once registered, users can log in with their credentials through a secure authentication interface. If the provided credentials match the stored records, the user is granted access to the system. Failed attempts due to incorrect input trigger informative error messages, guiding users

to rectify their input. This module ensures that only authorized users can access the system's features, thereby maintaining data confidentiality and preventing misuse.

Upon successful login, users are directed to the Home Page, which serves as the central navigation hub of the application. The home interface presents a simple and intuitive layout, providing users with an overview of the system's capabilities. It welcomes users with a personalized greeting and offers easy access to key functionalities such as the prediction system, account settings, and past usage history (if implemented). The design is focused on usability and smooth transitions, making it convenient even for non- technical users to interact with the system. Additionally, the Home Page may display system status messages, important alerts, or a brief summary of the CollusiveHijack detection process.

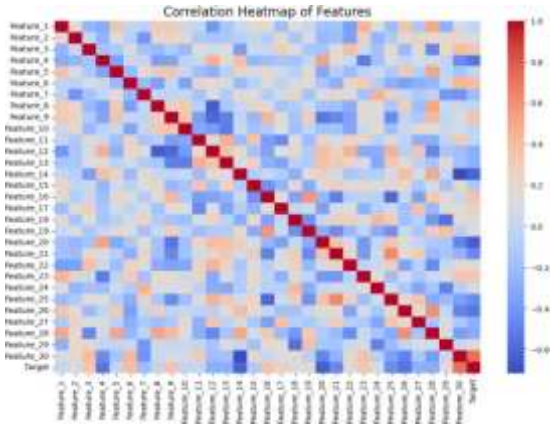
The most critical functionality lies in the Prediction Page, where the core analytical operations are performed. This module allows users to input relevant data values either manually or through uploading a dataset. These values typically include metrics such as packet delays, Inter-Contact Times (ICTs), and other network features needed for evaluating the presence of malicious routing behavior. Once the data is entered, the system applies statistical analysis—specifically the Kolmogorov- Smirnov two-sample test—to compare the observed delay distribution with the expected distribution derived from ICTs. Based on this comparison, as well as advanced detection strategies such as Path Detection Technique (PDT), Hop Detection Technique (HDT), or Early Hop Detection Technique (EHDT), the system predicts whether the route has been hijacked or remains unaffected. The result is displayed to the user as either "Route Hijacked" or "Route Safe," possibly along with a probability score or justification to enhance interpretability. For ease of use, the Prediction Page also includes options to clear input fields, submit new predictions, or view visual plots comparing expected and actual packet behavior.

In summary, the system integrates user- friendly modules with robust detection mechanisms to offer a reliable tool for identifying route hijacking in OMNs. Each module plays a vital role in ensuring seamless user interaction, secure access, and accurate real-time threat detection.

VI. RESULT

The proposed system was rigorously evaluated through extensive simulations and a proof-of-concept implementation to validate its effectiveness in detecting CollusiveHijack attacks in Opportunistic Mobile Networks (OMNs). The primary objective was to determine whether falsified Inter-Contact Times (ICTs) could be reliably identified using statistical methods and customized detection techniques.

The system successfully utilized the Kolmogorov-Smirnov (K-S) two-sample test to detect discrepancies between the expected packet delay distributions (derived from legitimate ICTs) and the observed delays in real-time network conditions. Based on this analysis, three detection techniques—Path Detection Technique (PDT), Hop Detection Technique (HDT), and Early Hop Detection Technique (EHDT)—were deployed and compared.



Experimental results demonstrate that the proposed methods are capable of accurately identifying route hijacking attacks with a detection rate ranging from 80.0% to 99.4%, particularly when the adversary Eve hijacked more than 60 packets. Among the three, the EHDT showed superior performance by offering early detection

capabilities, significantly reducing the time required to identify malicious activity. EHDT achieved a detection latency of 7 to 14 hours, which represents a 75% to 85% improvement compared to PDT and HDT. This reduction in latency enables quicker countermeasures and better system responsiveness.

Additionally, the system maintained a low false positive rate of approximately 3.6%, ensuring that benign behaviors were not incorrectly flagged as attacks. This balance of high detection accuracy and low false alarms indicates the practical viability of the system in real-world OMN scenarios. The prediction interface developed as part of the implementation allowed users to input routing data and instantly receive feedback on whether the communication path had been compromised. The intuitive user experience and clear output results made the system accessible even to users without deep technical expertise.

Overall, the results confirm that the integration of statistical validation with specialized detection strategies provides an effective defense mechanism against CollusiveHijack attacks in OMNs. The proposed solution not only strengthens network resilience but also contributes significantly to the field of secure mobile networking.

VII. CONCLUSION

This project successfully demonstrates a robust approach to detecting route hijacking attacks in Opportunistic Mobile Networks (OMNs), specifically targeting the CollusiveHijack threat. By leveraging the Kolmogorov-Smirnov two-sample test alongside tailored detection techniques such as PDT, HDT, and EHDT, the system effectively identifies malicious behavior based on discrepancies in packet delay distributions. The implementation not only achieves high detection accuracy but also maintains a low false positive rate, proving its reliability in practical scenarios.

The Early Hop Detection Technique (EHDT), in particular, offers significant improvements in detection speed, allowing for quicker identification of compromised routes. With an intuitive interface and efficient backend analysis, the system provides users with real-time insights into potential network threats, contributing to the development of secure and resilient routing in delay-tolerant mobile environments.

REFERENCES

[1] C. Yang and R. Stoleru, “Hybrid routing in wireless networks with diverse connectivity,” in *Proc. 17th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2016, pp. 71–80.

[2] S. Datta and S. Madria, “Efficient photo crowdsourcing with evolving POIs under delay-tolerant network environment,” *Pervasive Mobile Comput.*, vol. 67, 2020, Art. no. 101187.

[3] Firechat: Google play store, 2022. [Online]. Available: https://play.google.com/store

[4] Y. Liu, “Performance and energy consumption analysis of a delay-tolerant network for censorship-resistant communication,” in *Proc. 16th ACM Int. Sympos. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 257–266.

[5] E. Harkavy and M. S. Net, “Utilizing reinforcement learning to autonomously mange buffers in a delay tolerant network node,” in *Proc. IEEE Aerosp. Confer.*, 2020, pp. 1–8.

[6] E. Tikhonov, D. Schneps-Schneppe, and D. Namiot, “Delay tolerant network protocols for an expanding network on a railway,” in *Proc. Int. Conf. Innov. Intell. Inform. Comput. Technol.*, 2020, pp. 1–16.

[7] J. Wu, Y. Guo, H. Zhou, L. Shen, and L. Liu, "Vehicular delay tolerant network routing algorithm based on Bayesian network," *IEEE Access*, vol. 8, pp. 18727– 18740, 2020.

[8] Y. Dong, F. Zhang, I. Joe, H. Lin, W. Jiao, and Y. Zhang, "Learning for multiple- relay selection in a vehicular delay tolerant network," *IEEE Access*, vol. 8, pp. 175602– 175611, 2020.

[9] E. Yaacoub, K. Abualsaud, T. Khattab, and A. Chehab, "Secure transmission of IoT mhealth patient monitoring data from remote areas using DTN," *IEEE Netw.*, vol. 34, no. 5, pp. 226–231, Sep./Oct. 2020.

[10] Distressnet-ng project, 2022. [Online]. Available: https://www.nist.gov/ctl/pscr/distressnet-ng-resilient-mobile-broadband- communication-and-edge-computing.