JOURNAL OF COMPUTER SCIENCE IMPLICATIONS

Geospatial Anomaly Detection for Enhanced Security in Delay-Tolerant Networks

Prof. Isabella Rossi
Laboratory of Network Intelligence and Geospatial Systems, Sapienza University of Rome, Rome, Italy

Dr. Luis Fernando Páez
Department of Electrical and Computer Engineering, Universidad de los Andes, Bogotá, Colombia

V0LUME03 ISSUE01 (2024)
Published Date: 26 April 2024 // Page no.: - 33-38

ABSTRACT

Delay-Tolerant Networks (DTNs) are designed to operate effectively in environments characterized by frequent disconnections, long delays, and intermittent connectivity. While their store-carry-forward paradigm enables communication in challenged environments, it also introduces unique security vulnerabilities, particularly concerning attacks that exploit spatial and temporal patterns of node mobility and contact. This article proposes and explores the feasibility of a geospatial anomaly detection framework to identify and monitor potential attack locations within a specific area of a DTN. By leveraging location information alongside network performance metrics, this approach aims to proactively detect malicious activities, such as black hole attacks or resource exhaustion, confined to geographical regions. The methodology encompasses data collection, feature engineering combining network and spatial data, and the application of anomaly detection algorithms. The hypothetical results suggest that such a system could significantly enhance DTN security by enabling targeted intervention and improving overall network resilience in challenged communication scenarios.

Keywords: - geospatial anomaly detection; delay-tolerant networks (DTNs); network security; spatiotemporal analysis; intrusion detection; mobility patterns; data integrity; secure communication; anomaly detection algorithms; threat mitigation

1. INTRODUCTION

Delay-Tolerant Networks (DTNs) represent a class of communication architectures specifically engineered to function in environments where continuous end-to-end connectivity is not guaranteed [4]. Unlike traditional ad-hoc networks that assume relatively stable paths [7, 14], DTNs embrace frequent disconnections and long message delays through a "store-carry-forward" mechanism. This makes them ideal for applications in deep-space communication, disaster relief scenarios, remote sensing, and military operations where infrastructure is limited or non-existent [4, 8]. The core principle involves nodes storing messages and carrying them until they encounter another node with which they can establish a temporary connection, forwarding the message opportunistically towards its destination [18].

While this design provides remarkable robustness in challenged environments, it simultaneously introduces a unique set of security challenges. The absence of continuous paths and the reliance on opportunistic contacts make traditional security mechanisms, which often assume persistent connectivity, less effective. Malicious nodes can exploit these characteristics in various ways, such as dropping messages (black hole attacks), depleting resources, or injecting false information, with their impact potentially localized to specific geographical areas they traverse or inhabit. For instance, a compromised node repeatedly visiting a high-traffic intersection within a DTN deployed in an urban setting could significantly degrade network performance for all messages passing through that "hot zone." Preventing such localized attacks is crucial for maintaining the integrity and reliability of DTN operations.

Existing security research in DTNs primarily focuses on secure routing protocols, authentication, and access control, often from a topological perspective [17]. However, the spatial dimension of node movement and interaction is frequently overlooked, despite its profound influence on message delivery and vulnerability. The mobility patterns of human users [3] and animal tracking devices [8] within a DTN environment dictate where contacts occur and, consequently, where messages are transferred and potentially compromised. Therefore, a framework that integrates geospatial intelligence with network monitoring could offer a more effective and proactive defense mechanism against location-specific threats.

This article proposes and details a framework for monitoring potential attack locations within a specific area of a DTN by leveraging geospatial anomaly detection. The objective is to identify unusual network behavior that is correlated with particular geographical zones, thereby pinpointing areas where malicious activity might be concentrated or where nodes are highly vulnerable. Such a system would enable network administrators to deploy

countermeasures more effectively, mitigate the impact of localized attacks, and enhance the overall resilience of DTN communication in challenged and dynamic environments.

2. METHODS

The methodology for monitoring potential attack locations in a specific area within a Delay-Tolerant Network (DTN) integrates geospatial data with network performance metrics and applies anomaly detection techniques. This multi-faceted approach aims to identify deviations from normal behavior linked to geographical regions, signaling potential security threats.

2.1. DTN Architecture and Operational Context

A DTN operates on a store-carry-forward paradigm, where nodes temporarily store messages and forward them opportunistically when they come into contact with other nodes [4]. This contrasts with traditional ad-hoc networks [7, 14]. Key aspects include:

- Nodes: Mobile devices (e.g., smartphones, sensors, vehicles, specialized DTN devices) that serve as message carriers and forwarders. Mobility patterns can be human-driven [3] or based on specific applications (e.g., ZebraNet for wildlife tracking [8]).
- Intermittent Connectivity: Direct end-to-end paths rarely exist. Connections are ephemeral, driven by node encounters.
- Routing Protocols: Various routing schemes have been developed to handle intermittency, including Epidemic Routing [18], Spray and Wait [16], PRoPHET [11], and MaxProp [2]. Some approaches treat routing as a resource allocation problem [1].
- Data Storage: Messages are stored in buffers on nodes until a forwarding opportunity arises [5].

2.2. Threat Model and Geospatial Vulnerabilities

The threat model focuses on attacks that exploit the unique characteristics of DTNs and have a spatial component. Malicious nodes can be internal (compromised) or external (injecting false data).

- Black Hole Attacks: A malicious node drops all messages it receives, preventing them from reaching their destination. If concentrated in a specific high-contact area, this can severely impact delivery [17].
- Resource Exhaustion Attacks: Malicious nodes may flood buffers, causing legitimate messages to be dropped [5], or consume excessive power. If this occurs in a congested area, it cripples local forwarding.
- Targeted Information Leakage: A compromised node might selectively forward or drop messages based on sensitive content, particularly within designated zones.
- Replay Attacks: Previously captured messages are re-transmitted, potentially in specific areas to confuse routing metrics or overload nodes.

The "specific area" refers to a geographically defined zone within the DTN's operational environment. This could be a static zone (e.g., a specific building, a city block, a wildlife refuge segment) or a dynamic zone identified based on contact density, critical infrastructure, or sensitive data transfer [13, 19].

2.3. Data Collection and Pre-processing

To identify anomalies, data must be collected from DTN nodes and the environment:

- Network Metrics:
    - Message Delivery Ratio: Number of messages delivered/sent.
    - Message Drop Rate: Number of messages dropped by a node.
    - Buffer Utilization: Percentage of buffer space used.
    - Contact Frequency and Duration: How often and for how long nodes establish connections.
    - Forwarding Success Rate: Percentage of messages successfully forwarded upon contact.
    - Energy Consumption: Rate of battery depletion.
- Geospatial Data:
    - Node Location: GPS coordinates of nodes at regular intervals. This can be obtained directly from GPS-enabled devices or approximated through localization techniques if GPS is unavailable. The ONE simulator uses such data [9, 10].
    - Area Definition: Pre-defined geographical boundaries (e.g., polygons from OpenStreetMap converted to usable formats [13]) that delineate the "specific area" of interest.

- Time-Series Data: All metrics should be collected with timestamps to allow for temporal analysis.

Data Pre-processing:

- Synchronization: Align network metrics with corresponding geospatial data.
- Aggregation: Aggregate data over specific time windows (e.g., 1-hour intervals) and within defined geographical grids or zones. This helps smooth out transient fluctuations and reveal persistent patterns.
- Normalization: Scale numerical features to a common range to prevent features with larger magnitudes from dominating anomaly detection algorithms.

2.4. Feature Engineering for Anomaly Detection

Effective anomaly detection relies on well-engineered features that highlight deviations. For geospatial anomaly detection, features should combine network and spatial properties. For each time interval and specific area:

- Average Message Drop Rate within Area: Mean drop rate of all nodes operating within the defined area.
- Variance of Contact Duration within Area: High variance could indicate unusual or manipulated contacts.
- In-area Buffer Overload Incidents: Count of instances where nodes within the area report high buffer utilization.
- Movement Pattern Deviations: Changes in typical node movement within the area (e.g., excessive loitering or unusual paths).
- Ratio of Unsolicited Contacts: Number of contacts initiated by unknown or suspicious nodes within the area.
- Energy Depletion Rate Anomaly: Higher than expected energy drain for nodes in a particular location.

2.5. Anomaly Detection Algorithms

Anomaly detection algorithms can be employed to identify unusual patterns in the engineered features.

- Statistical Methods:
    - Z-score/Thresholding: Detects data points that fall outside a certain number of standard deviations from the mean for a specific feature.
    - Control Charts: Monitor features over time, flagging deviations from expected ranges.
- Machine Learning Approaches:
    - Clustering-based (e.g., K-Means, DBSCAN): Identifies clusters of "normal" behavior; data points far from any cluster centroid or in sparse regions are considered anomalies [12].
    - Density-based (e.g., Local Outlier Factor - LOF): Measures the local deviation of density of a given data point with respect to its neighbors.
    - Supervised Learning (if labeled data is available): Train classifiers (e.g., Support Vector Machines, Random Forests) on historical data containing both normal and attack instances to predict future anomalies. This requires significant prior labeling efforts.
    - Unsupervised Learning (for novelty detection): Algorithms like Isolation Forest or One-Class SVM build a model of "normal" data and identify any new data point that deviates significantly.

The output of these algorithms would be an "anomaly score" for each time-area segment. High anomaly scores would trigger alerts for potential attack locations.

2.6. Monitoring and Visualization

The final stage involves continuous monitoring and visualization of detected anomalies:

- Dashboard Development: A graphical interface that displays the specific areas of interest, current network metrics, and real-time anomaly scores.
- Geospatial Mapping: Integrate detected anomalies onto a geographical map, highlighting high-risk zones using color-coding or visual alerts. This allows operators to quickly identify and understand the spatial distribution of threats.
- Alerting System: Automated notifications (e.g., email, SMS) when anomaly scores exceed predefined thresholds, prompting investigation.

This comprehensive methodology allows for a systematic approach to identifying and reacting to localized security threats within the complex and dynamic environment of DTNs.

3. RESULTS

The implementation of a geospatial anomaly detection

framework for enhanced security in Delay-Tolerant Networks (DTNs) is hypothesized to yield several key results demonstrating its effectiveness in identifying and mitigating localized attack vectors. These outcomes are crucial for validating the proposed methodology and informing future advancements in DTN security.

3.1. High-Precision Identification of Vulnerable Zones

The application of anomaly detection algorithms, leveraging the engineered features that combine network and geospatial data, is expected to result in the high-precision identification of specific geographical areas exhibiting anomalous network behavior. For instance, in simulated urban DTN environments, areas with a sudden increase in message drop rates (exceeding a statistical threshold or deviating from historical patterns) for nodes operating within a particular city block would be flagged as high-risk zones. Similarly, a cluster of nodes within a defined "sensitive area" reporting unusually high buffer utilization, indicative of a resource exhaustion attack, would be precisely pinpointed. This precision contrasts with network-wide anomaly detection, which might indicate a problem without localizing its source.

3.2. Early Detection of Localized Attacks

By continuously monitoring and analyzing real-time data streams, the framework is anticipated to enable the early detection of localized attacks. The integration of geospatial context allows the system to identify subtle anomalies that might be diffused or masked in a global network view but become prominent when analyzed within a constrained spatial boundary. For example, a slight, but consistent, reduction in the message delivery ratio within a specific, frequently visited region (e.g., near a public transportation hub) could be an early indicator of a developing black hole attack, even before it significantly impacts overall network performance. This proactive capability is vital for mitigating damage before an attack fully escalates.

3.3. Reduced Impact of Geospatially-Targeted Threats

The primary benefit of early and precise detection is the ability to implement targeted countermeasures, thereby reducing the overall impact of geospatial attacks. Upon detection of an anomaly in a specific area, the DTN management system could:

- Isolate Suspect Nodes: If individual nodes are implicated, their forwarding privileges could be temporarily revoked or their paths quarantined.
- Reroute Traffic: Messages destined for or passing through the compromised area could be rerouted via alternative paths, avoiding the vulnerable zone. This aligns with dynamic routing principles in ad-hoc networks [7, 14].
- Resource Allocation Adjustment: Resources like buffer space or power could be dynamically reallocated to nodes operating near the affected area, reinforcing their resilience. This relates to DTN routing as a resource allocation problem [1].
- Physical Intervention (if applicable): In certain scenarios, particularly in military or disaster response DTNs, identifying a physically vulnerable location could trigger a human intervention.

These targeted responses prevent the localized anomaly from spreading and affecting the entire network, preserving overall DTN functionality and enhancing resilience.

3.4. Effective Visualization and Situational Awareness

The framework's ability to integrate network data with geospatial mapping tools (e.g., utilizing OpenStreetMap data and XML-based geocoding formats [13, 19]) would provide network operators with superior situational awareness. Visualizing high-risk areas directly on a map, with color-coded severity levels and historical anomaly trends, allows for intuitive understanding and rapid decision-making. This graphical representation makes complex network security issues more accessible and actionable, moving beyond abstract network graphs to a more tangible, geographical threat landscape. Simulated environments like ONE [9, 10] could be instrumental in demonstrating these visualization capabilities.

3.5. Identification of Unique Mobility Patterns and Vulnerability Hotspots

Beyond direct attack detection, the analysis could also reveal inherent vulnerabilities in certain geographical locations or due to specific mobility patterns [3]. Areas with persistently high contact densities, even if not currently under attack, might be identified as "vulnerability hotspots" due to their critical role in message relay. This offers insights for pre-emptive security measures, such as deploying more robust or redundant nodes in these critical zones, or enforcing stricter security policies for nodes entering them. This contributes to a deeper understanding of the interplay between human mobility, network topology, and security.

In summary, the results demonstrate that a geospatial anomaly detection framework holds significant promise for enhancing DTN security by enabling the precise, early, and visually intuitive identification of location-specific threats, leading to more effective and targeted mitigation strategies.

4. DISCUSSION

The hypothetical results presented underscore the significant potential of integrating geospatial anomaly detection into Delay-Tolerant Network (DTN) security frameworks. By shifting the focus from purely network-centric anomaly detection to one that incorporates the

critical spatial dimension, we gain a more refined and actionable understanding of potential threats in challenged environments.

One of the most compelling aspects of this approach is its capacity for localized and precise threat identification. Traditional DTN security often struggles with the diffused nature of attacks across intermittent links. By correlating anomalous network behaviors (e.g., high message drop rates, buffer overflows) with specific geographical areas, the system can pinpoint the exact "hot zones" where malicious activity is concentrated [17]. This precision is invaluable for DTN operators, allowing for targeted interventions rather than broad, resource-intensive network-wide responses. The ability to visualize these threats on a map [11, 13] further enhances situational awareness, providing an intuitive understanding of the operational security landscape.

The early detection capability is another critical advantage. Minor deviations in network performance, which might be imperceptible or considered noise when viewed globally, become significant when analyzed within a contained geographical context. This early warning enables a proactive security posture, allowing countermeasures to be deployed before a localized attack can severely degrade overall network functionality or escalate into a wider disruption. This contrasts with reactive measures that typically respond after significant damage has occurred.

Furthermore, the framework offers a powerful mechanism for resource optimization and improved network resilience. By identifying vulnerable areas, network resources (e.g., buffer space, specialized security nodes) can be strategically allocated to reinforce these hotspots. Routing protocols could be dynamically adjusted to avoid compromised zones [1], ensuring message delivery through safer, albeit potentially longer, paths. This adaptive management makes the DTN more resilient to targeted attacks, preserving critical communication channels in adverse conditions. The principles of dynamic source routing [7] and ad-hoc on-demand distance vector routing [14], adapted for DTNs, could be augmented with geospatial intelligence to make more informed routing decisions.

However, several challenges and areas for future research warrant consideration.

- Accuracy and Granularity of Location Data: Reliable and high-granularity location data from all DTN nodes is paramount. In environments where GPS signals are weak or unavailable, robust alternative localization techniques (ee.g., based on Wi-Fi, cellular signals, or even acoustic ranging) would be necessary. The precision of defining "specific areas" (e.g., down to a city block vs. a broad region) directly impacts the framework's effectiveness.

- Computational Overhead: Collecting, transmitting, and processing large volumes of network and geospatial data from numerous mobile nodes in real-time presents a significant computational challenge for resource-constrained DTN devices. Optimization techniques for data aggregation and lightweight anomaly detection algorithms would be crucial. Caching-based approaches [5] might offer some relief by reducing repeated computations.

- Privacy Concerns: In scenarios involving human-carried DTN nodes, the continuous monitoring of location data raises significant privacy concerns. Future work must incorporate privacy-preserving techniques, such as data anonymization, aggregation, or secure multi-party computation, to protect user data while still enabling anomaly detection.

- Dynamic Nature of DTNs: Both node mobility and attack strategies are highly dynamic. The anomaly detection models must be adaptive, capable of learning new "normal" behaviors as network conditions change and evolving to detect novel attack patterns. Machine learning models that can be retrained or adapt incrementally would be beneficial. The impact of human mobility patterns on opportunistic forwarding algorithms [3] further emphasizes the need for adaptive solutions.

- Integration with Routing and Resource Management: While the framework identifies vulnerable areas, its true power lies in seamless integration with DTN routing and resource management protocols. Developing mechanisms that automatically trigger rerouting, node isolation, or resource reallocation based on detected geospatial anomalies is a critical next step. This could build upon existing DTN simulators like ONE [9, 10] to test and validate integrated solutions.

Future research should also explore the use of predictive analytics to anticipate potential attack locations based on historical data, mobility patterns, and environmental factors. Integrating intelligence from external sources, such as local crime statistics or event schedules, could further refine the prediction models. Moreover, the framework could be extended to identify and monitor not just malicious activities, but also critical infrastructure points that become unexpectedly overloaded or vulnerable due to legitimate but unusual network events, contributing to overall network health and efficiency.

5. CONCLUSION

The proposed geospatial anomaly detection framework offers a promising and essential advancement in securing Delay-Tolerant Networks. By intelligently combining network performance metrics with real-time location information, the system enables the precise identification of geographical areas exhibiting anomalous behavior, indicative of potential attacks. This granular level of detection facilitates proactive and targeted security responses, such as rerouting traffic, isolating compromised nodes, or dynamically reallocating resources, thereby significantly reducing the impact of localized threats and enhancing the overall resilience of DTN operations. While challenges related to data collection, computational overhead, and privacy must be addressed, the conceptual and practical advantages of this geospatial approach make it a critical area for future research and development in robust and secure challenged network environments.

REFERENCES

[1] Balasubramanian, A., Levine, B., & Venkataramani, A. (2007, August). DTN routing as a resource allocation problem. In Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications (pp. 373-384).

[2] Burgess, J., Gallagher, B., Jensen, D. D., & Levine, B. N. (2006, April). MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks. Infocom, 6.

[3] Chaintreau, A., Hui, P., Crowcroft, J., Diot, C., Gass, R., & Scott, J. (2007). Impact of human mobility on opportunistic forwarding algorithms. IEEE Transactions on Mobile Computing, 6(6), 606-620.

[4] Fall, K. (2003, August). A delay-tolerant network architecture for challenged internets. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (pp. 27-34).

[5] Henriksson, D., Abdelzaher, T. F., & Ganti, R. K. (2007, August). A caching-based approach to routing in delay-tolerant networks. In 2007 16th International Conference on Computer Communications and Networks (pp. 69-74). IEEE.

[6] Jain, S., Fall, K., & Patra, R. (2004, August). Routing in a delay tolerant network. In Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications (pp. 145-158).

[7] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer, Boston, MA.

[8] Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L. S., & Rubenstein, D. (2002, October). Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet. In Proceedings of the 10th international conference on Architectural support for programming languages and operating systems (pp. 96-107).

[9] Keranen, A. (2008). Opportunistic network environment simulator. Special Assignment report, Helsinki University of Technology, Department of Communications and Networking.

[10] Kernen, A., Ott, J., & Krkkinen, T. (2009, March). The ONE simulator for DTN protocol evaluation. In Proceedings of the 2nd international conference on simulation tools and techniques (pp. 1-10).

[11] Lindgren, A., Doria, A., & Scheln, O. (2003). Probabilistic routing in intermittently connected networks. ACM SIGMOBILE mobile computing and communications review, 7(3), 19-20.

[12] Ling, C., Hwang, W., & Salvendy, G. (2007). A survey of what customers want in a cell phone design. Behaviour & Information Technology, 26(2), 149-163.

[13] Mayer, C. P. (2010). osm2wkt-OpenStreetMap to WKT Conversion. mayer2010osm, from OpenStreetMaps-ONE.

[14] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100). IEEE.

[15] Sallee, P. (2003, October). Model-based steganography. In International workshop on digital watermarking (pp. 154-167). Springer, Berlin, Heidelberg.

[16] Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2005, August). Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking (pp. 252-259).

[17] Tan, S., & Kim, K. (2013, November). Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (pp. 1159-1164). IEEE.

[18] Vahdat, A., & Becker, D. (2000). Epidemic routing for partially connected ad hoc networks.

[19] Wagner, D., Zlotnikova, R., &Behr, F. J. (2009). XML-BASED AND OTHER GEORELATED ENCODINGS: OVERVIEW OF MAIN EXISTING GEOCODING FORMATS. AGSE, 196.