Network Hexagons Under Attack: Secure Crowdsourcing of Georeferenced Data

***Abstract*—A critical requirement for modern Intelligent Transportation Systems (ITS) is the secure and anonymous collection of georeferenced data from connected vehicles and mobile devices. The Nexagon protocol, leveraging the Locator/ID Separation Protocol (LISP) and the H3 geo-spatial indexing system, provides a promising foundation for privacy-preserving, real-time data aggregation. However, significant security and privacy vulnerabilities persist in its current form. This work systematically analyzes these vulnerabilities using the STRIDE and LINDDUN threat modeling frameworks, revealing risks such as user reidentification, session linkage, and sparse-region attacks. To address these, we propose an enhanced architecture combining public key infrastructure (PKI) with ephemeral pseudonym certificates, randomized key rotation, and adaptive geospatial resolution. Our prototype, deployed as a microservice-based overlay, demonstrates that these mitigations can be implemented with less than 25% increase in latency and under 7% throughput reduction, validating their practicality for real-world ITS deployment.**

I. Introduction

The proliferation of connected vehicles and mobile devices enables large-scale crowdsourcing of georeferenced data, promising transformative improvements in transportation efficiency and safety. Real-time data from distributed edge devices supports applications such as traffic optimization, hazard detection, and infrastructure monitoring. However, the collection and aggregation of such sensitive data raise significant privacy and security concerns, particularly regarding user anonymity and protection against tracking or data compromise. The Nexagon protocol, under development by the IETF, utilizes LISP for network addressing and H3 for spatial indexing, enabling efficient, location-based data aggregation. Despite its potential, the protocol lacks robust authentication and privacy mechanisms, motivating a systematic threat analysis and the design of practical mitigations. [1]–[4].

II. System Architecture and Threat Analysis

Nexagon organizes mobile edge devices into hierarchical hexagonal tiles using H3, with LISP providing separation of endpoint identifiers and routing locators for scalable network management. Key components include authentication nodes, geo-mapping nodes, and aggregation nodes (Fig. 2). To assess privacy and security, we decomposed the architecture into data flow diagrams and applied STRIDE and LINDDUN frameworks, mapping threats to system elements (Table I). This analysis identified critical vulnerabilities, including:

- **Sparse-region attacks**: While hexagons offer an efficient approach to localizing data from mobile clients, privacy concerns arise when H3 tiles are overlaid on road networks in sparsely populated or remote areas. In such regions, the low density of clients can inadvertently expose individuals to privacy risks. As illustrated in Figure 2, a lone client moves from Point **A** to Point **B** along a defined road with overlaid hexagonal tiles. As the client provides periodic updates, its position within the grid can be easily tracked. Each time the client enter a new hexagon, its presence can be easily noticed, making it a trivial task to infer the client's direction and ultimately predict the final destination.
- **Session linkage and re-identification**: Static identifiers and insufficient pseudonymity expose users to tracking across sessions. An attacker could identify users by correlating pseudonyms with external datasets.
- **Spoofed agent attacks**: Malicious actors may attempt to disrupt the service discovery process or compromise client privacy during device initialization by impersonating a legitimate authentication server.

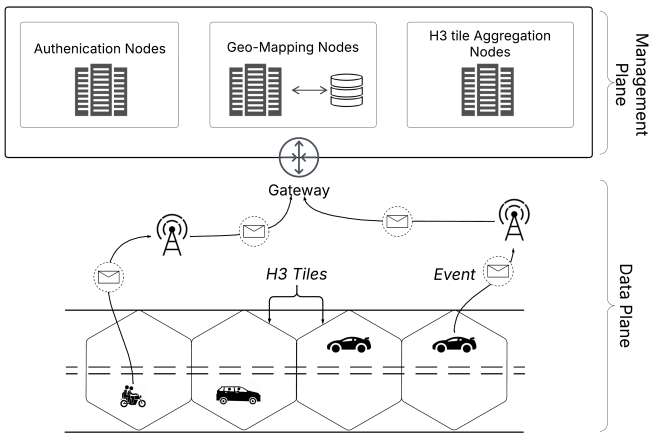


Fig. 1. An Overview of the Nexagon protocol architecture.

Mitigations include dynamic adjustment of H3 resolution, randomized EID and certificate rotation, and hardware-backed attestation for device authentication.

III. Implementation and Evaluation

We implemented the enhanced Nexagon protocol as a microservice overlay, with each agent encapsulated in a containerized service. The authentication system operates as a root CA, issuing pseudonym certificates with frequent key rotation. Mobile clients periodically swap endpoint identifiers and certificates, preserving anonymity even under active surveillance. Mapping and aggregation agents process and store data streams, supporting scalable analytics. Performance

TABLE I
THREATS, AFFECTED COMPONENTS, ATTACK DESCRIPTIONS, AND MITIGATIONS IN NETWORK HEXAGONS

Threat	**Affected Component(s)**	**Attack Description**	**Mitigation**	**Risk Level**
Session Linkage	–Mobile Client –Authentication Agent	An attacker links users by connecting credentials across different processes and tracking actions across sessions through static identifiers or similar patterns.	–Use pseudonymized EIDs that are rotated dynamically. –Add dummy traffic to prevent timing-based correlation.	High
User Re-identification	–Mobile Client –Mapping Agent	An attacker identifies users by correlating pseudonyms with external datasets (for example IP addresses).	–Authenticate users without revealing identity. –Encrypt all metadata in communications and storage or use an onion router.	Medium
Sparse Region Attack	–Mobile Client	An attacker exploits sparsely populated or remote areas by leveraging the low density of clients within static hexagonal grids.	–Expand hexagonal regions dynamically in sparse areas. –Ensure at least k clients are indistinguishable in any region.	High
Client Request/Response Replay	–Authentication Agent –Mapping Agent	An attacker replays valid authentication requests to bypass non-repudiation mechanisms.	–Include nonces in requests to prevent replay attacks. –Use mutual TLS (mTLS) for bidirectional verification.	Medium
Spoofed Agent	–Mobile Client –Mapping Agent	An attacker impersonates a legitimate client or authentication agent.	–Use hardware-backed attestation for device verification. –Require both parties to authenticate each other using certificates.	High

High - Very strong likelihood of occurring and has a critical effect on the Nexagons, and **Not** currently addressed by well-known schemes
Medium - Very strong likelihood of occurring, has a critical effect on the Nexagons, and currently addressed by well-known schemes
Low- Very weak likelihood of occurring and has a critical effect on the Nexagons

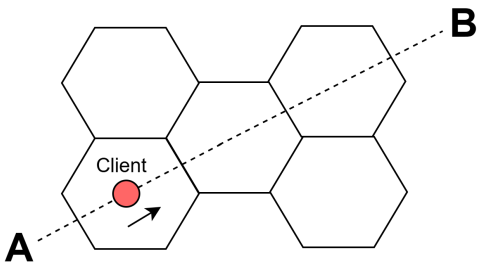


Fig. 2. A mock scenario illustrating a lone clients roaming within sparsely populated hexagons.

evaluation was conducted in a virtualized testbed simulating edge device requests. Key results (Table III) show that the proposed security extensions increase average latency by 25% and reduce throughput by less than 7%, remaining within acceptable operational limits for ITS applications.

IV. DISCUSSION

Our findings demonstrate that robust privacy and security for georeferenced crowdsourcing in ITS can be achieved with modest performance overhead. The combination of PKI, pseudonym certificates, and adaptive geospatial resolution effectively mitigates reidentification, linkage, and sparse-region risks. Next steps include deploying the prototype in real-world vehicular networks to empirically assess metrics under sustained load.

V. CONCLUSION

This work delivers a comprehensive threat analysis and practical security enhancements for the Nexagon protocol, enabling secure, privacy-preserving crowdsourcing of georeferenced data in ITS. Our prototype validates the feasibility of these solutions for large-scale, real-time deployment. Future work will focus on real-world evaluation and experiment with running distributed AI on Nexagons for efficient task-offloading in vehicular networks.

REFERENCES

[1] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 383–398, 2019.

[2] J. Liu, H. Shen, H. S. Narman, W. Chung, and Z. Lin, "A survey of mobile crowdsensing techniques: A critical component for the internet of things," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 2, Jun. 2018.

[3] IETF Working Group, *draft-ietf-lisp-nexagon-54*, Internet Engineering Task Force, Sep. 2024.

[4] A. Rodriguez-Natal, M. Portoles-Comeras, V. Ermagan, *et al.*, "Lisp: A southbound sdn protocol?" *IEEE Communications Magazine*, vol. 53, no. 7, pp. 201–207, 2015.

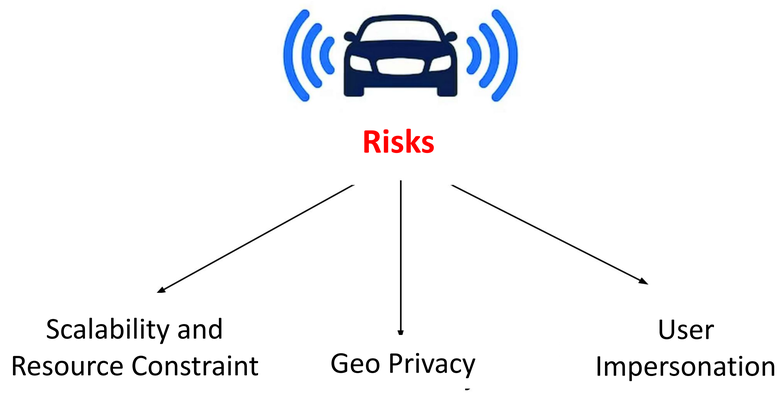
Carnegie Mellon University Africa

Secure Crowdsourcing of Geo-Referenced Data using Nexagons

Okemawo Obadofin [1], João Barros [1]
[1] Carnegie Mellon University Africa, Kigali, Rwanda

Problem: Unsecure Connected Vehicles

- Crowdsourcing data from connected vehicles presents unique challenges in privacy and security.
- Addressing these risks is critical to ensuring user trust and safeguarding data integrity.



How do we guarantee privacy for users of connected vehicles?

Why do we need to crowdsource data from connected vehicles?

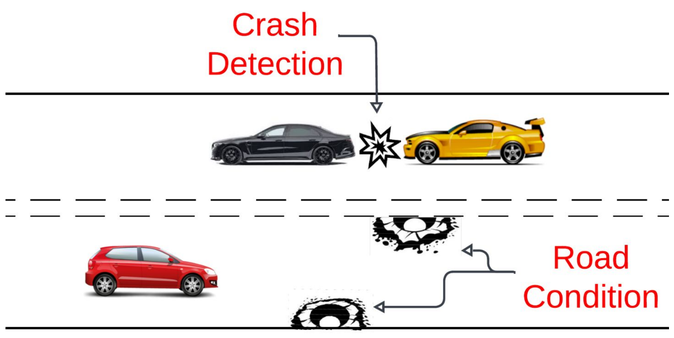


Fig: Enhancing Safety with Connected Vehicles: Crash Detection and Road Condition Monitoring Use Cases

Our Solution

- The Nexagon (Network Hexagon) protocol conceptualizes a real-time network for geospatial mapping using the hierarchical hexagonal (H3) library and distributed agents.
- Vehicles use Euphemeral IDs, and HID (Hexagon IDs) are used to localize data instead of gps traces.

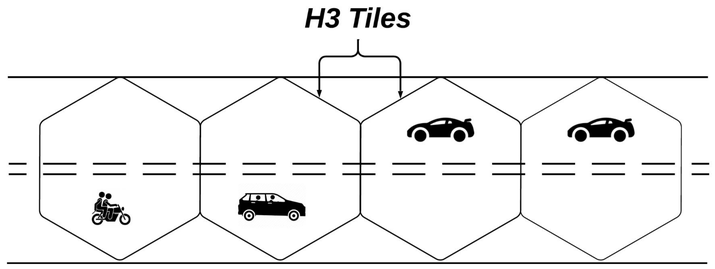


Fig: Network Hexagons

Our extension guarantees user privacy by:

- Varying encryption keys and client ID
- Software TPM to verify mobile edge nodes
- Pseudonym Certificates issued by a trusted Certificate Authority (CA)

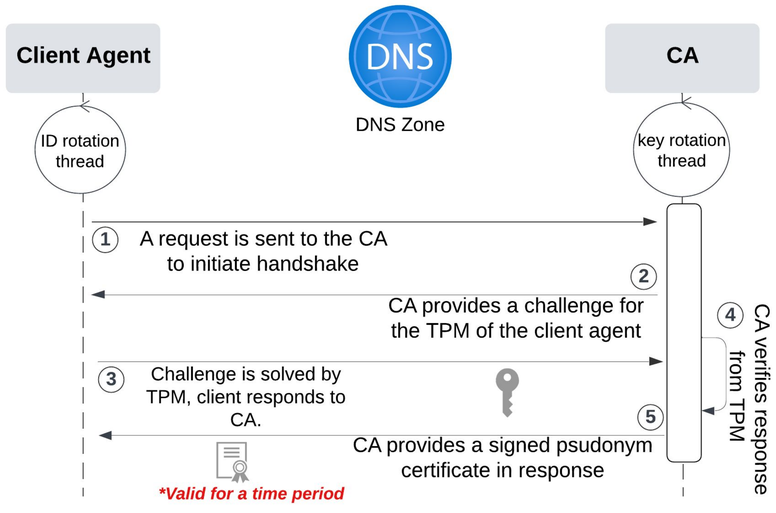
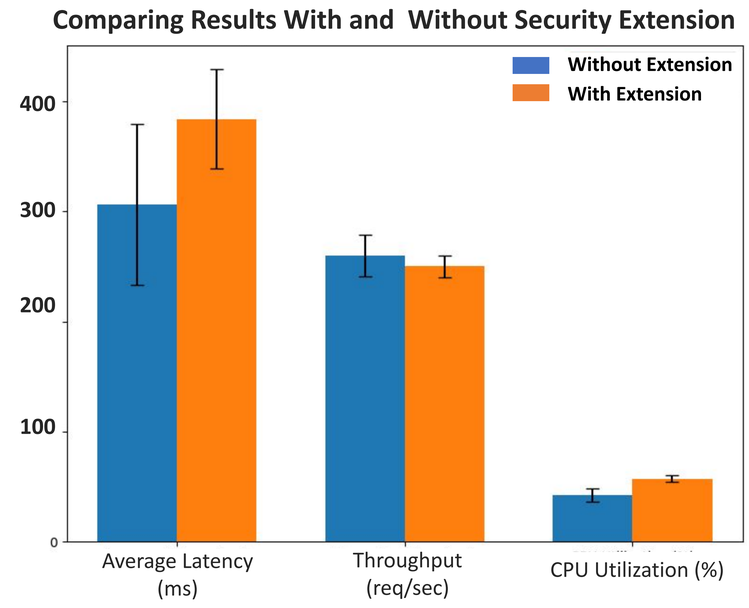


Fig: Authentication flow for clients in the Nexagon protocol

Results

- We leveraged STRIDE and LINDDUN threat modelling frameworks to establish a list of critical attacks.

Threat	Mitigation
Spoofed Agent	Authenticate users without revealing identity.
User Re-identification	Use hardware-backed attestation for device verification.
Sparse Region Attack	Expand hexagonal regions dynamically in sparse areas.



Ongoing Research

- Experimenting with distributed AI applications for efficient off-loading in mobility systems
- Formulate mathematical models that confirm the systems anonymity guarantees.

References

[1] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges,"
[2] IETF Working Group, draft-ietf-lisp-nexagon-54, Sep. 2024.
[3] V. Uher, P. Gajdos, V. Sn ˇ a´sel, Y.-C. Lai, and M. Radecky, "Hierarchical hexagonal clustering and indexing,"