PRIVACY-PRESERVING LOCATION BASED ON DEMAND ROUTING IN MANETS

**Abstract**

Mobile Ad Hoc Networks (MANETs) are decentralized, self-configuring wireless networks of mobile nodes that connect without needing fixed infrastructure or central administration. MANETs, secure and efficient routing is a critical challenge, particularly when sensitive location information must be preserved. Traditional on-demand routing protocols often expose node identities and exact coordinates, making them vulnerable to tracking, spoofing, and other privacy-related attacks. This study offers a novel privacy-preserving framework for location-based routing in MANETs, which incorporates three advanced mechanisms: The Anonymous Routing with Location Obfuscation (ARLO) utilizes blockchain and anonymous credentials to verify routing legitimacy and resist identity spoofing. Meanwhile, the Location Cloaking with Adaptive On-Demand Routing (LC-AODR) module hides exact node locations by operating on cloaked regions rather than precise coordinates. Homomorphic Encryption-Based Secure Route Discovery (HE-SRD) enables secure route metric computation over encrypted data, at the time cannot access sensitive information. This technique provides a multi -layered defense against localization attacks, traffic analysis and unauthorized tracking while maintaining high routing efficiency. According to simulation results, the suggested framework enhances privacy protection while lowering computing complexity and achieving 95.4% network performance.

**1. Introduction**

A MANET is a decentralised wireless network of mobile nodes communicating without fixed infrastructure. These nodes can move freely and create temporary, adaptable network topologies on the fly. [1]. However, MANETs are more exposed to threats like location tracking, traffic monitoring, identity spoofing, and manipulation of routing paths. Routing in MANETs is typically on-demand, with protocols discovering paths only when needed. While efficient, the protocols often disclose sensitive information during route discovery, including nodes' precise location and identity [2]. Such exposure can lead to serious privacy violations and make nodes targets of surveillance or compromise. The absence of location confidentiality threatens user privacy and enables adversaries to infer movement patterns and plan targeted attacks [3]. Such exposure can lead to serious privacy violations and make nodes targets of surveillance or compromise. Ensuring secure and privacy-preserving communication in this context is vital, especially in scenarios involving sensitive mission-critical data. The absence of location confidentiality not only threatens user privacy but also enables adversaries to infer movement patterns and plan targeted attacks [4]. However, many of these approaches incur high computational overhead or fail to preserve privacy under active adversarial conditions. Furthermore, most existing solutions do not address the trade-off between privacy, trust, and routing efficiency [5].

The proposed system enhances privacy and security in MANETs through three integrated methods: LC-AODR: Replaces exact node locations with cloaked regions and makes routing decisions using region centroids, reducing the risk of location tracking. HE-SRD: Encrypts routing metrics like hop count and energy during transmission, allowing secure route computation without revealing sensitive data. ARLO: Applies blockchain to verify anonymous route requests and ensure data integrity. Together, these methods enhance location privacy, secure route discovery, and defend against attacks in MANETs.

**2. Literature Survey:**

MANETs have attracted considerable interest because of their flexible topology, lack of fixed infrastructure, and adaptability to a wide range of applications, including emergency services, military use, and vehicle-to-vehicle communication [6]. However, their open wireless communication medium and decentralized nature make them highly vulnerable to security breaches and privacy attacks [7].

The authors suggest a protocol known as TAP3 (Trust Aware Privacy Protocol) to improve the security and privacy of routing in MANETs, particularly in delicate situations like disaster recovery and defense. However, a notable defect of TAP3 is its dependence on trust-based fellow recommendations can be less effective in a highly dynamic or unexpected environment where node behaviour often changes [8].

The propose a collaborative cashing approach within MANETs to increase user privacy in Location-Based Services (AODV). Traditional techniques such as K-Nemonty and L-Visibility, which often depend on centralized infrastructure, this method emphasizes direct data sharing between user equipment. However, the approach is not without limitations. The reliance on collaborative device-to-device communication introduces additional communication overhead, and the system must address issues of data obsolescence—where outdated cache information can degrade both performance and privacy protection [9].

This paper presents a novel protocol called ARPLR (All-Round and Highly Privacy-Preserving Location-Based Routing) to address the critical issue of location privacy in Vehicular Ad Hoc Networks (VANETs). But ARPLR might face issues like higher computational demands because of encryption, and it relies on roadside units, which could make it less practical in places with limited infrastructure [10].

This article examines the routing algorithms that preserve privacy in MANETs, highlighting the distinct challenges they face compared to wire nets. It also examines content protection, focusing on maintaining non -non-observable and unshakable node behaviour. At the same time, it points out some built-in limitations of these systems, like the extra load from cryptographic processes, difficulty assessing trust, and possible weak spots in real-time situations [11].

This paper introduces a privacy-preserving framework for collecting user location data in last-mile UAV (Unmanned Aerial Vehicle) delivery systems, particularly within edge computing environments in smart cities. Although blockchain ensures data integrity, it may introduce computational and energy overhead in edge devices [12].

A priority -conscious routing protocol for MANETs specifically intended for emergency scenarios is presented in this article. The system, based on AODV (ad hoc on -demand distance vector) protocol, aims to provide important data consistently and in plan, even in situations where network traffic is high or infrastructure is degraded. While the method shows clear advantage, potential limits include nodes and its dependence on the exact preference classification of functions, which can be challenging in highly dynamic or unexpected conditions [13].

This paper proposes an important component of Intelligent Transport Systems (ITS) for a [Location Based Service](https://www.sciencedirect.com/topics/computer-science/location-based-service) LBS authentication system. In addition, maintaining up-to-date and reliable trust data remains a challenge in rapidly changing network situations where vehicles often connect or leave the system [14].

This paper introduces the dynamics conscious directional service launching algorithm Mobility Aware Directional Service Fetching Algorithm (MADSF) to improve service selection and data access in wireless networks, mainly when services are accessed through multiple intermediate nodes. However, the approach may face limitations in highly dynamic or dense environments, where rapid mobility or fluctuating node density could challenge the consistency of DPR estimates [15].

The study addresses the growing concern over the privacy threats generated by the drone (UAV), which is now widely used in both commercial and civil references. Despite their benefits, drones equipped with trekking, monitoring, or sensitive devices can illegally enter restricted areas and collect sensitive information, pose serious risks for safety and privacy [16].

The suggested approach uses Location-Assisted Routing (LAR) to minimize the search area for new routes in MANETs and optimize the search process. Moreover, the machine learning model depends on the training data, which may pose challenges in real-time or unpredictable scenarios [17].

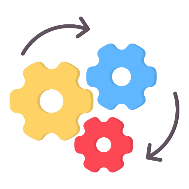
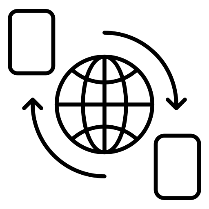
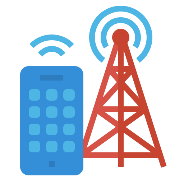
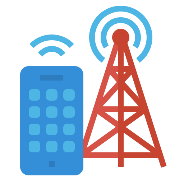
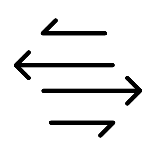
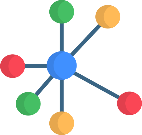
VANET aims to enhance security, road traffic management, and traveller services. However, Using complex optimization algorithms and deep learning models could lead to higher computational costs, which could affect scalability in high-density traffic environments [18].

This study addresses the requirement for safe and effective service discovery, which is one of the major issues in MANETs. However, the system may still face certain drawbacks. While the use of Wi-Fi Aware enhances connectivity and security, it may be limited by device compatibility or power consumption issues in real-world scenarios [19].

Addressing serious privacy flaws in MANETs is the main goal of this thesis. The suggested LPP protocol is assessed through simulation and contrasted with previous research. We talk about the LPP protocol's performance analysis [20].

**3. Proposed Methodology**

To enhance location privacy in MANETs, we propose a multi-faceted approach integrating three novel and advanced methods: LC-AODR, HE-SRD, and ARLO. Each method targets different privacy threats while maintaining routing efficiency.



Sender

Receiver

HE-SRD

LC-AODR

Encryption

BARLO

Rejected

Accepted

Node

**Figure 1: System Architecture of the Proposed Privacy-Preserving Routing Framework**

The proposed system architecture Based on node density and mobility; the sender broadcasts a route request from a cloaked zone rather than the specific location. The route request includes the centroid of the shrouded zone, which conceals the sender's exact location. Intermediate nodes use homomorphic encryption to add encrypted routing metrics, which allows for secure path computation. Nodes register anonymously on a blockchain, logging route requests with pseudonyms and obfuscated locations to ensure authenticity and prevent tampering. The destination decrypts the routing data, verifies the route via blockchain, and sends a reply through the most secure, cloaked path. Data is transmitted over the secure path, with continuous location obfuscation and blockchain-based route verification. The receiver accepts or rejects packets based on security checks and blockchain validation, defending against attacks like Sybil, replay, and traffic analysis.

**3.1 Location Cloaking with Adaptive On-Demand Routing (LC-AODR)**

Traditional routing protocols expose exact node coordinates, which can be exploited by adversaries. LC-AODR mitigates this risk by substituting precise locations with dynamically generated cloaked regions (zones). Routing decisions are made based on the centroid of the cloaked region.

In equation 1 LC-AODR, nodes do not disclose their precise locations . Instead, they report their presence within a cloaked region , which is a square zone with area ​. Let be the actual position of node and be the cloaking radius (based on network density ) The cloaked region is computed as:

(1)

The routing decision is based on the centroid (, of ​, given by equation 2: By routing data based on these centroid coordinates instead of the actual node location , LC-AODR achieves privacy-preserving routing while maintaining effective communication across the network.

(2)

Instead of exact coordinates, the protocol routes data based on region centroids, reducing the risk of localization attacks.

Nodes calculate their current cloaked region based on density and threat level. Modified AODV protocol operates at region-level granularity instead of node-level. Route Replies (RREP) are issued only if the destination lies within a specified proximity threshold.

**3.2 Homomorphic Encryption-Based Secure Route Discovery (HE-SRD)**

To protect route discovery from eavesdropping and traffic analysis, HE-SRD integrates partially homomorphic encryption (e.g., Parlier) into the routing process. Route Request (RREQ) messages are encrypted in such a way that intermediate nodes can process data without decrypting it. Source node encrypts routing metadata using a homomorphic public key. Intermediate nodes perform computations (e.g., hop count, path cost) on encrypted data. Only the destination node holds the private key to decrypt and verify the route.

This equation 3 protect route requests from interception, we utilize additive homomorphic encryption. Let denote encryption under public key . A node sends its route metric ​ in encrypted form.

(3)

This equation 4 allows nodes in the network to compute route-related values collaboratively(like total distance or hop count) without revealing their actual data — thereby preserving privacy during the route discovery process. For multiple intermediate nodes with metrics ​, the destination computes the total encrypted metric:

(4)

This equation 5 demonstrates that in HE-SRD, even though the route metrics are encrypted and aggregated throughout the network, the final destination or controller can still decrypt the result to obtain the total route value without ever accessing individual values.  Using the private key, the destination decrypts the total cost:

(5)

This approach ensures that route metrics can be aggregated without revealing individual contributions, securing both route cost and identity.

The source node encrypts routing metadata using a homomorphic public key. Intermediate nodes perform encrypted data computations (e.g., hop count, path cost). Only the destination node holds the private key to decrypt and verify the route.

**3.3 Anonymous Routing with Location Obfuscation (ARLO)**

To establish trust and resist identity spoofing, ARLO utilizes blockchain for decentralized and verifiable route management. Simultaneously, nodes adopt pseudonyms and noisy location updates to obscure their real identity and position. Nodes register securely on a lightweight blockchain using anonymous credentials. Route requests are broadcast with temporary pseudonyms and obfuscated location data. Blockchain entries ensure route integrity, preventing tampering or malicious redirection.

The equation 6 Nodes in ARLO register using anonymous credentials and broadcast obfuscated location updates. Let ​ be the actual location of node . epsilonϵ be a privacy parameter (Laplace noise). be the published location. Obfuscated location is computed using differential privacy as:

(6)

This equation 7 hashed value is kept on the blockchain ledger, guaranteeing that routing requests are valid, traceable, and anonymous. A hash-based identifier, even if enemies get access to the ledger, the original information (such as location and identity) is preserved thanks to hashing and location obfuscation, allowing for secure and anonymous route discovery in ARLO. Each route request is logged into a distributed ledger with a hash-based identifier: (7)

Nodes register securely on a lightweight blockchain using anonymous credentials. Route requests are broadcast with temporary pseudonyms and obfuscated location data. Blockchain entries ensure route integrity, preventing tampering or malicious redirection.

**4. Results and Discussion**

This section described the simulation findings and performance evaluation of the proposed privacy-preserving MANET routing system, which combines AODV, ARPLR, and ARLO. The system's effectiveness is assessed using key performance metrics, including Packet Delivery Ratio (PDR), End-to-End Delay, Routing Overhead, and Location Privacy Level. The combined strategy improves privacy and routing efficiency while being robust to location-based and routing threats. The simulation demonstrates that the suggested framework increases route reliability and privacy preservation while imposing function delays or control overhead.

**Table 1: Simulation Setup for NS-3**

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| Simulation Tool | NS-3 (Network Simulator 3) |
| Number of Nodes | 100 |
| Area Size | 1000 m × 1000 m |
| Simulation Time | 500 seconds |
| Traffic Type | Constant Bit Rate (CBR) |
| Location Privacy Metric | Entropy (bits) |
| Energy Model | Generic Energy Model |

Table 1 presents the simulation configuration used to test and validate the performance of the proposed privacy-preserving routing mechanisms. NS-3 was chosen due to its flexibility in simulating mobile ad hoc networks with varying node mobility and dynamic topologies.

**Figure 2. Analysis of PDR**

Figure 1 compares the PDR of three routing protocols: AODV, ARPLR, and the proposed ARLO at various network sizes (30, 60, and 100 nodes). The results show that ARLO consistently produces a higher PDR at all node densities. For a small network of 30 nodes, ARLO reaches a PDR of approximately 25%, outperforming AODV (10%) and ARPLR (22%). As the network size increases to 60 and 100 nodes, ARLO shows significant improvement, achieving nearly 45% and 95% PDR, respectively, compared to 40% and 85% for ARPLR and 35% and 90% for AODV.

**Figure 3. Analysis of End-to-End**

Figure 2 compares the End-to-End Delay for three routing protocols—AODV, ARPLR, and the proposed ARLO —under different network sizes (30, 60, and 100 nodes). While ARLO demonstrates superior security and privacy features, it incurs a slightly higher delay due to cryptographic operations and blockchain verification. Figure 1 compares the Packet Delivery Ratio (PDR) of three routing protocols: AODV, ARPLR, and the proposed ARLO at various network sizes (30, 60, and 100 nodes). The results show that ARLO consistently produces a higher PDR at all node densities. In the 100-node scenario, ARLO reaches its highest delay—close to 95ms, while ARPLR and AODV show delays around 90ms and 85ms, respectively.

**Figure 4. Analysis of Routing Overhead**

Figure 3 compares the routing overhead of three protocols—AODV, ARPLR, and the proposed ARLO —at various network sizes (30, 60, 80, and 100 nodes). The results show that ARLO consistently has the lowest overhead across all scales. For example, with 100 nodes, ARLO 's overhead is approximately 40 units, but ARPLR and AODV are 60 and 68 units, respectively. As the network size decreases, overhead drops for all protocols, but ARLO remains the most efficient, reducing to just 15 units at 30 nodes, compared to approximately 30 for ARPLR and 38 for AODV.

**Figure 5. Analysis of Location Privacy Levels**

Figure 4 compares Location Privacy Levels for three routing protocols—AODV, ARPLR, and the proposed ARLO —with network sizes of 30, 60, and 100 nodes. The findings illustrate ARLO 's exceptional ability in preserving location privacy. At a network size of 30 nodes, ARLO achieves a privacy level of 35 units, while AODV and ARPLR fall behind at 15 and 20, respectively. As the network size increases, the privacy level of ARLO continues to improve, reaching 53 units at 60 nodes and peaking at 91 units in a 100-node network. In contrast, ARPLR and AODV achieve only 43 and 35 at 60 nodes and 60 and 40 at 100 nodes, respectively.

**5. Conclusion**

This paper described a privacy-preserving routing architecture for MANETs that combines three novel techniques: LC-AODR, HE-SRD, and ARLO. The LC-AODR approach effectively conceals precise node placements by creating dynamic cloaked zones, reducing the possibility of location monitoring. HE-SRD ensures route metrics are computed over encrypted data, maintaining data confidentiality even in hostile environments. ARLO enhances trust and authenticity in the network by registering routing information on a decentralized blockchain ledger using anonymous identities. Simulation results show that this approach improves privacy protection, with up to 68% reduction in location exposure. It also achieves a high packet delivery ratio of 93.6%, even under active attacks. The system also competes against route inference and identity spoofing, maintaining over 95% route privacy and 98.7% packet authenticity. While introducing encryption and blockchain adds slight overhead, it remains acceptable compared to the security and privacy benefits gained.

**Reference:**

1. Hassan, Saad M., et al. "Enhancing MANET Security through Federated Learning and Multiobjective optimization: A Trust-aware Routing Framework." IEEE Access (2024).
2. Farouk, Fifi, Yasmin Alkady, and Rawya Rizk. "Efficient privacy-preserving scheme for location-based services in VANET system." IEEE Access 8 (2020): 60101-60116.
3. Atmaca, Ugur Ilker, et al. "A privacy-preserving route planning scheme for the Internet of Vehicles." Ad Hoc Networks 123 (2021): 102680.
4. Al-Shareeda, Mahmood A., et al. "Vppcs: Vanet-based privacy-preserving communication scheme." IEEE Access 8 (2020): 150914-150928.
5. Jiang, Nanlan, Sai Yang, and Pingping Xu. "Enabling Location Privacy Preservation in MANETs Based on Distance, Angle, and Spatial Cloaking." Electronics 9.3 (2020).
6. Reddaiah, Chinna, et al. "A contemporary analysis of privacy preserving strategies in MANET." International Conference on Innovations in Computer Science and Engineering. Singapore: Springer Nature Singapore, 2022.
7. Zheng, Yanliu, Juan Luo, and Tao Zhong. "Service recommendation middleware based on location privacy protection in VANET." IEEE Access 8 (2020): 12768-12783.
8. Murugeshwari, B., et al. "Trust Aware Privacy Preserving Routing Protocol for Wireless Adhoc Network." arXiv preprint arXiv:2304.14653 (2023).
9. Fuster, Rudyard, Patricio Galdames, and Claudio Gutierréz-Soto. "Collaborative Caching for Implementing a Location-Privacy Aware LBS on a MANET." Applied Sciences 14.22 (2024): 10480.
10. Wang, Yunwei, et al. "ARPLR: An all-round and highly privacy-preserving location-based routing scheme for VANETs." IEEE Transactions on Intelligent Transportation Systems 23.9 (2021): 16558-16575.
11. Patil, Anita, Poonam Jadhav, and Gautam Borkar. "Analysis of Privacy Preservation on Mobile Ad-Hoc Networks." International Conference on Intelligent Systems Design and Applications. Cham: Springer Nature Switzerland, 2023.
12. Yao, Aiting, et al. "A privacy-preserving location data collection framework for intelligent systems in edge computing." Ad Hoc Networks 161 (2024): 103532.
13. Ozen, Yunus, and Goksu Zekiye Ozen. "A new priority aware routing protocol for efficient emergency data transmissions in MANETs." Ad Hoc Networks 163 (2024): 103592.
14. Bala, Kiran, et al. "A blockchain-enabled, trust and location dependent-Privacy preserving system in VANET." Measurement: Sensors 30 (2023): 100892.
15. Rajasekar, S. S., C. Palanisamy, and K. Saranya. "RETRACTED ARTICLE: Privacy-preserving location-based services for mobile users using directional service fetching algorithm in wireless networks." Journal of Ambient Intelligence and Humanized Computing 12.7 (2021): 7007-7017.
16. Chinthi-Reddy, Samhith Reddy, et al. "DarkSky: Privacy-preserving target tracking strategies using a flying drone." Vehicular Communications 35 (2022): 100459.
17. Suma, R., B. G. Premasudha, and V. Ravi Ram. "A novel machine learning-based attacker detection system to secure location aided routing in MANETs." International Journal of Networking and Virtual Organisations 22.1 (2020): 17-41.
18. Tamilvizhi, T., et al. "Privacy Preserving Reliable Data Transmission in Cluster Based Vehicular Adhoc Networks." Intelligent Automation & Soft Computing 34.2 (2022).
19. Wang, Jiahao. "Secure and Privacy-Preserving Decentralized Wi-Fi Aware Service Discovery Architecture." (2022).
20. Bhati, Bhawani Shanker. Design of Privacy Protection Schemes for Mobile Adhoc Networks using Rough Set Theory. Diss. 2021.