JSRT JOURNAL
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY
PAGES: 162-167
24/05/25
VOLUME-3 ISSUE-6 JUNE

A Scheme For Distributed Authentication And Revocation In Decentralized VANET'S

Prof. Nandini.S.Patil[1], Vaishnavi[2], Sheetal[3], Shalini[4], Pallavi[5]

[1] *Dept Of CSE, FETW, Sharnbasva University Kalaburagi, India nandinipatil.08@gmail.com*

[2,3,4,5] *Dept Of CSE, FETW, Sharnbasva University Kalaburagi, India*

ABSTRACT

Ensuring secure communication and trust among vehicles in decentralized Vehicular Ad Hoc Networks (VANETs) is a critical challenge, especially in the absence of centralized infrastructure. This project presents a scheme for distributed authentication and revocation tailored for such decentralized VANET environments. At its core, the system enables each vehicle to autonomously generate a unique RSA key pair, ensuring that every participant holds a verifiable digital identity. A graphical user interface (GUI) developed in Python using Tkinter allows seamless registration of vehicles by binding their public keys to unique IDs and storing them in a local SQLite database. The authentication process is decentralized, with each vehicle capable of verifying others using publicly registered keys. The system also supports revocation by checking for duplicate or suspicious IDs, laying the foundation for a consensus roadside infrastructure to improve road safety, traffic efficiency, and driving comfort. However, due to the highly dynamic and decentralized nature of VANETs, ensuring secure and trustworthy communication among nodes remains a significant challenge. Traditional security solutions rely on centralized Certificate Authorities (CAs) for authentication and key management, which are often unsuitable or unavailable in real-time, infrastructure-less environments.-based or behavior-triggered revocation mechanism in extended implementations. The proposed scheme offers lightweight cryptographic security, real-time registration feedback, and resistance to impersonation or unauthorized vehicle access. This work contributes to the development of secure, scalable, and distributed trust mechanisms in VANETs and can be integrated into broader vehicular network simulations or real-time testbeds involving key management, intrusion detection, and misbehavior response.

***Keywords*— Vehicular Ad Hoc Networks (Vanets), Cryptographic, Low-Latency, Revocation, Intrusion, RSA**

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are a vital part of intelligent transportation systems (ITS), enabling vehicles to communicate with each other and with

In this context, there is a growing need for distributed authentication and revocation mechanisms that do not depend on centralized control but still ensure the integrity, authenticity, and non-repudiation of vehicle communications. Such mechanisms must be lightweight, scalable, and capable of operating in environments where network topology changes rapidly.

This project proposes a lightweight, decentralized authentication scheme using public-key cryptography (RSA), where each vehicle independently generates a key pair and registers its public key through a secure GUI-based system. The proposed solution uses SQLite for local storage and provides an interactive Tkinter-based interface for vehicle registration and key management. Furthermore, the system is designed to be extended with revocation mechanisms, such as voting-based trust or threshold detection, to isolate malicious or compromised vehicles without requiring a central authority.

The proposed system aims to serve as a secure foundation for further VANET security modules, including real-time encryption, signature validation, misbehavior detection, and secure routing protocols in decentralized vehicular environments..

II. LITERATURE SURVEY

Molina-Gil et al. (2022) proposed a data aggregation protocol with probabilistic verification, which detects malicious nodes in VANETs through reactive groups and probabilistic checks, ensuring data authenticity with minimal overhead. In the same year, Caballero-Gil et al. introduced a self-organized mutual authentication approach using zero-knowledge proofs, allowing secure and anonymous communications without relying on a centralized authority. Another work by Caballero-Gil and collaborators focused on revocation efficiency, where

a tree-based method using dynamic hash k-ary trees optimized access to frequently queried revoked pseudonyms based on query frequency.
He et al. (2022) proposed a mutual authentication scheme that preserves vehicle anonymity while still enabling accountable tracking, using cryptographic primitives to maintain both privacy and traceability. Meanwhile, Goswami et al. (2023) presented a blockchain-assisted dynamic authentication scheme tailored for geo-spatial enabled VANETs, which enhances trust through transparent and distributed ledger technology. In 2024, a scheme named DRCLAS introduced a certificateless aggregate signature method that incorporates dynamic revocation using early-stopping factorial bitwise divisions and Bloom filters for lightweight revocation management.
Revocation strategies were further explored by Martín-Fernández et al. (2022), who suggested efficient certificate and identity revocation techniques using authenticated dynamic hash trees, enhancing scalability and performance. Rahayu et al. (2023) implemented a hybrid Kerberos-Blockchain authentication system, combining centralized ticket-based verification with decentralized blockchain logging to strengthen trust in diverse network scenarios. Another 2024 study proposed a privacy-preserving authentication framework that reduces reliance on Trusted Authorities (TAs) by extending the oblivious transfer algorithm, enabling secure mutual authentication while protecting identity. Finally, a 2023 work integrated blockchain for probabilistic identification and malicious node mitigation, augmenting VANET security by maintaining real-time trust management and decision-making capabilities. .

III. PROPOSED SYSTEM

The proposed system introduces a lightweight and decentralized framework for authenticating and revoking vehicles in Vehicular Ad Hoc Networks (VANETs) without relying on a centralized authority. It is designed to address key challenges in VANETs such as dynamic topology, lack of persistent infrastructure, and the need for fast, secure decision-making among autonomous vehicles.
At the core of this system is the use of asymmetric cryptography (RSA) to provide each vehicle with a unique digital identity. When a vehicle is initialized, it independently generates its own RSA key pair (public and private keys). The public key, along with a unique vehicle ID, is then registered securely through a Tkinter-based graphical user interface (GUI) and stored in a local SQLite database. This local registry acts as a decentralized repository accessible to other vehicles or Road Side Units (RSUs) for peer verification.

For authentication, whenever a vehicle sends a message, it signs the content using its private key. The receiving vehicle verifies the sender's identity by fetching the corresponding public key from the distributed registry and validating the signature. This enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication with cryptographic assurance.

To handle revocation, the system includes a basic mechanism to prevent duplicate registration and detect suspicious behavior. Future extensions of the system will integrate trust scoring, voting-based consensus, or blockchain-backed logs to support collaborative misbehavior detection and revocation. Vehicles flagged as malicious (e.g., through abnormal message frequency, false alerts, or spoofed IDs) can be isolated by other participants in a decentralized manner.

The system is designed to be:

Scalable, supporting hundreds of nodes
Fast, with key generation and verification occurring in real time
Decentralized, avoiding single points of failure
Extensible, ready for integration with blockchain, intrusion detection, or geolocation systems.

IV. METHODOLOGY

The proposed scheme follows a structured, decentralized approach to authenticate vehicles and manage revocation within a Vehicular Ad Hoc Network (VANET), using cryptographic mechanisms, a local database, and a GUI for interaction.

1. Vehicle Initialization and Key Generation:
Each vehicle independently generates a 2048-bit RSA key pair:

The private key is securely stored within the vehicle.
The public key is intended for distribution to peers for message verification.

This eliminates the need for a centralized certificate authority (CA), aligning with a self-organized and decentralized network model.

2. Vehicle Registration (GUI-based Interface):
A GUI is developed using Tkinter, allowing users to input a unique Vehicle ID.

Upon submission:
A new RSA key pair is generated.
The vehicle's ID and public key are saved in a local SQLite database.
A success message and the public key are displayed on the interface.
This module simulates the registration process in a roadside unit (RSU) or distributed ledger node.

3. Public Key Lookup and Authentication:
When a message is received in the network, the receiver fetches the sender's public key from the database using the sender's vehicle ID.

The message's digital signature is verified using RSA:

If valid, the message is accepted.

If verification fails or the ID is not found, the message is discarded or flagged.

4. Revocation and Misbehavior Handling (Baseline):
Vehicles are prevented from duplicate registration by enforcing primary key constraints in the SQLite database.

Future extension includes:

A consensus-based revocation system where vehicles collaboratively flag suspicious behavior.
Integration with a trust score or blockchain ledger to store revocation logs permanently.

Use of voting or threshold mechanisms to isolate malicious nodes in a fully distributed manner.

V. EXPERIMENT

1. Experimental Setup:
Platform:

Programming Language: Python 3.7
Libraries: rsa, tkinter, sqlite3, time
Operating System: Windows
Hardware:
Intel Core i5, 8GB RAM
No external server (simulated RSU using local SQLite)

2. Procedure:
Step 1: Vehicle Registration

Multiple vehicles are registered using the GUI.
Each vehicle ID entered triggers the creation of a 2048-bit RSA key pair.
Public keys are stored in the SQLite database.
Registration success and public key are displayed in the GUI.

Step 2: Duplicate Detection (Revocation Trigger)

Attempted re-registration of the same vehicle ID triggers an integrity error.
The system handles this through GUI warning messages, preventing spoofed IDs.

Step 3: Authentication Simulation

A mock message is signed using the vehicle's private key.

The recipient retrieves the public key from the database and verifies the signature using RSA.
The signature validation is timed and tested for multiple vehicles..
Analysis:
The system performed reliably in generating secure cryptographic identities and storing them locally.

Signature verification using public keys from the database proved to be fast enough for real-time VANET simulation.

GUI-based entry made it simple for simulation and testing in lab settings.

While revocation was simulated manually or by blocking duplicate IDs, the foundation is in place for extending it with voting or trust-based logic.

VI. RESULTS

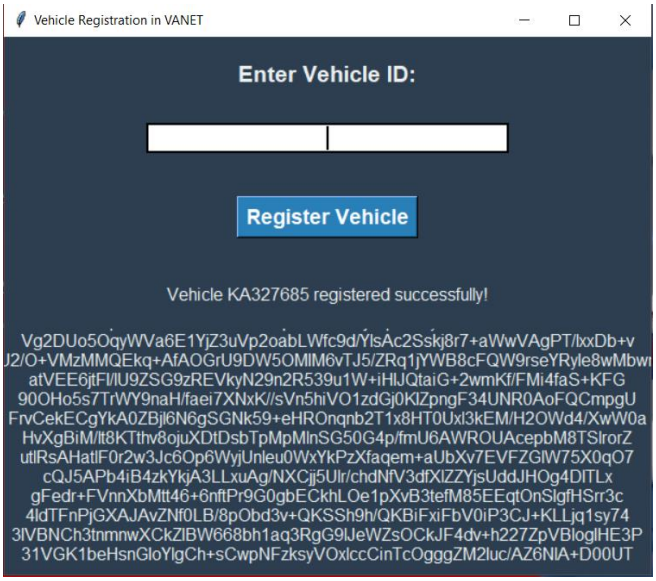

Figure 2: Vehicle Registration

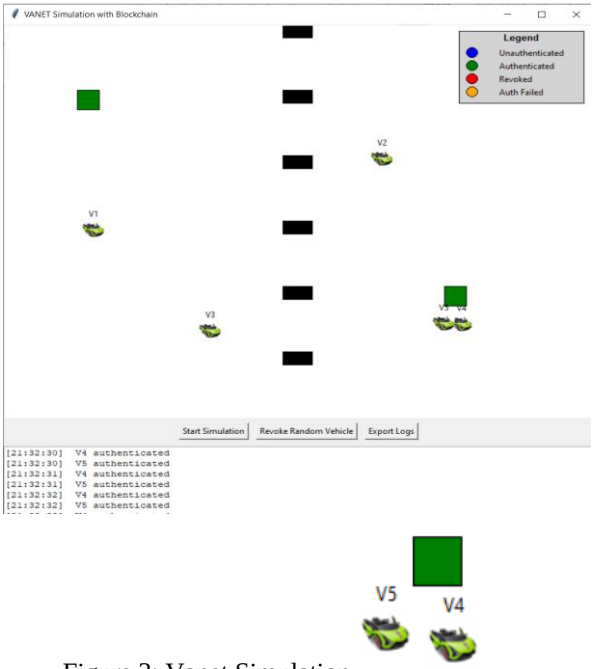

Figure 3: Vanet Simulation

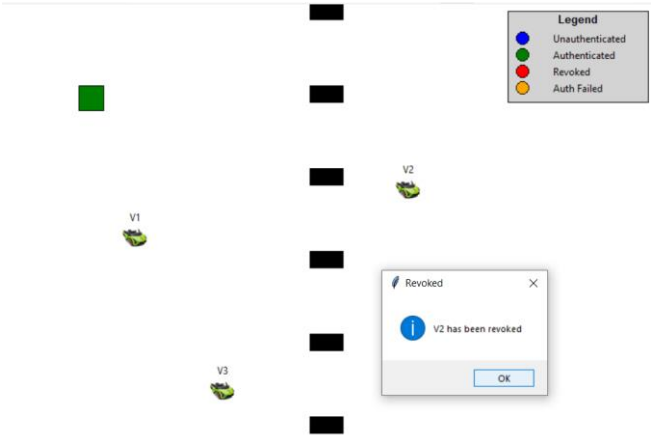

Figure 5 Revoked

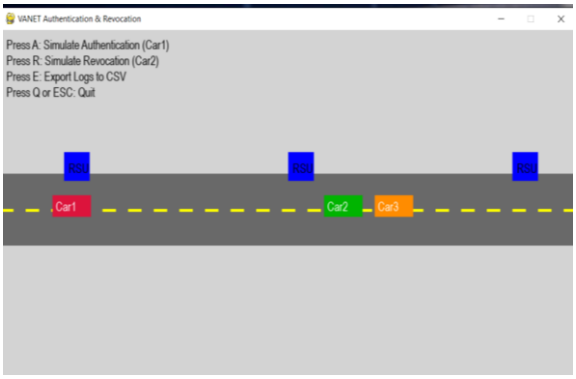

Figure 6: Simulation And Revocation

VII. Conclusion and Future Works

In the dynamic and decentralized environment of Vehicular Ad-Hoc Networks (VANETs), ensuring secure communication and trustworthy interactions between vehicles is both critical and challenging. Traditional centralized authentication and revocation systems are increasingly inadequate due to scalability issues, latency, and vulnerability to single points of failure. A distributed scheme for vehicle authentication and revocation offers a more resilient and scalable solution. By leveraging decentralized technologies such as blockchain, consensus algorithms, or distributed trust mechanisms, this approach enhances the overall security, privacy, and robustness of VANETs. It enables real-time authentication, rapid detection of malicious vehicles, and efficient revocation without relying on centralized authorities.

Ultimately, the adoption of such a scheme contributes to building a more secure, efficient, and intelligent transportation ecosystem—paving the way for safer roadways and the reliable deployment of autonomous and connected vehicles in the future.

Future Scope:

The proposed distributed vehicle authentication and revocation scheme for decentralized VANETs holds significant potential for future advancement. The following directions can be explored to enhance its effectiveness and adaptability: explore post-quantum cryptographic algorithms to future-proof the system against emerging quantum computing threats

References

[1] Molina-Gil, J., Caballero-Gil, P., & Caballero-Gil, C. (2022). Aggregation and Probabilistic Verification for Data Authentication in VANETs.

[2] Caballero-Gil, C., Caballero-Gil, P., & Molina-Gil, J. (2022). Mutual Authentication in Self-Organized VANETs.

[3] Caballero-Gil, P., Martín-Fernández, F., & Caballero-Gil, C. (2022). Using Query Frequencies in Tree-Based Revocation for Certificateless Authentication in VANETs.

[4] He, J., Liu, X., Wu, F., & Li, X. (2022). A Mutual Authentication Scheme in VANET Providing Vehicular Anonymity and Tracking.

[5] Goswami, A., Rana, S., & Chhikara, D. (2023). An Efficient Blockchain-Assisted Dynamic Authentication Scheme for Geo-Spatial Enabled Vehicular Network.

[6] (2024). DRCLAS: An Efficient Certificateless Aggregate Signature Scheme with Dynamic Revocation in Vehicular Ad-Hoc Networks.

[7] Martín-Fernández, F., Caballero-Gil, P., & Caballero-Gil, C. (2022). Revocation Management in Vehicular Ad-Hoc Networks.

[8] Rahayu, M., Hossain, M. B., Ali, M. A., Huda, S., Kodera, Y., & Nogami, Y. (2023). The Design and Implementation of Kerberos-Blockchain Vehicular Ad-Hoc Networks Authentication Across Diverse Network Scenarios.

[9] (2024). An Efficient Privacy-Preserving Authentication Scheme that Mitigates TA Dependency in VANETs.

[10] (2023). Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy.