**Cooperative approach for data-centric and node-centric misbehavior detection in VANET**

**. Introduction**

* **What is VANET?**

In the present era, Cooperative Intelligent Transportation Systems (C-ITS) have immensely contributed towards road safety, optimizing traffic management and offering entertainment services to individuals on the road. These services are facilitated by Vehicular Ad Hoc Networks (VANET), establishing connections through Vehicle to Everything (V2X) communication among autonomous vehicles, pedestrians and Road Side Units (RSU), including traffic lights, cameras and access point.

* **Why privacy (pseudo identities) → Sybil attack risk?**

vehicles use pseudo identities (fake names/IDs) to preserve their driver privacy

which makes it vulnerable to sybil attacks.

A **Sybil attack** is attack where one malicious vehicle creates multiple fake identities to spread misleading information.

* **Why Sybil attack is dangerous (fake congestion, disrupts safety & traffic apps)**

it creates **fake congestion** and disrupts **safety and traffic applications** in VANET.

**Problem Statement**

* In VANET, vehicles use pseudo identities for privacy, but attackers exploit this to launch Sybil attacks by creating multiple fake identities. Existing methods only detect Sybil behavior locally and cannot link multiple Sybil identities together to the real attacker which make Hard to catch the actual attacker. The challenge is to detecting Sybil attacks is hard because fake identities can send plausible messages. . There is a need for a framework that help to link multiple Sybil identities together and can accurately detect, connect, and revoke Sybil nodes both locally and at the RSU level

**Limitations of Existing Work**

**Local Detection**

* **Local = at one vehicle or within a small neighborhood of vehicles.**
* Problem: If a Sybil attacker controls multiple fake IDs in the same region, their messages can support each other and still look **plausible** which make detection hard. detection stays **limited to a single spot**, without knowing what happens in the wider vanet.

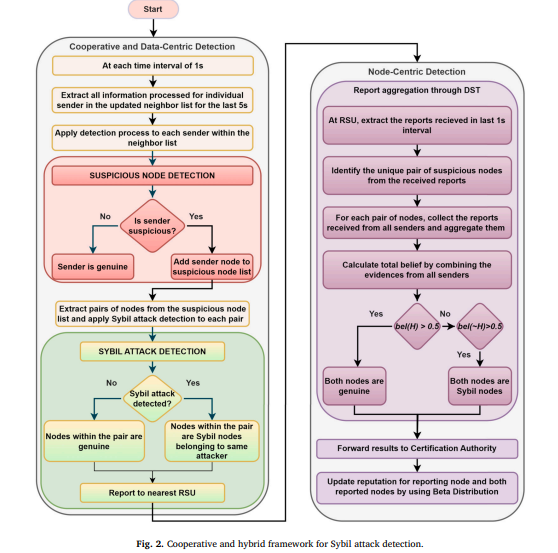
**Global Connections**

* **Global = across multiple Road Side Units (RSUs) or the whole VANET network.**
* Idea: Even if Sybil nodes look fine locally, their identities and movement patterns may show **links** when observed across different RSUs. For example, the same fake identities may reappear at different locations, moving in suspiciously identical patterns.

**Objectives**

Verify detections at **RSU level** using cooperative node-centric approach and

Improve detection in **real-time traffic scenarios** compared to existing methods.

**Proposed Framework:** 

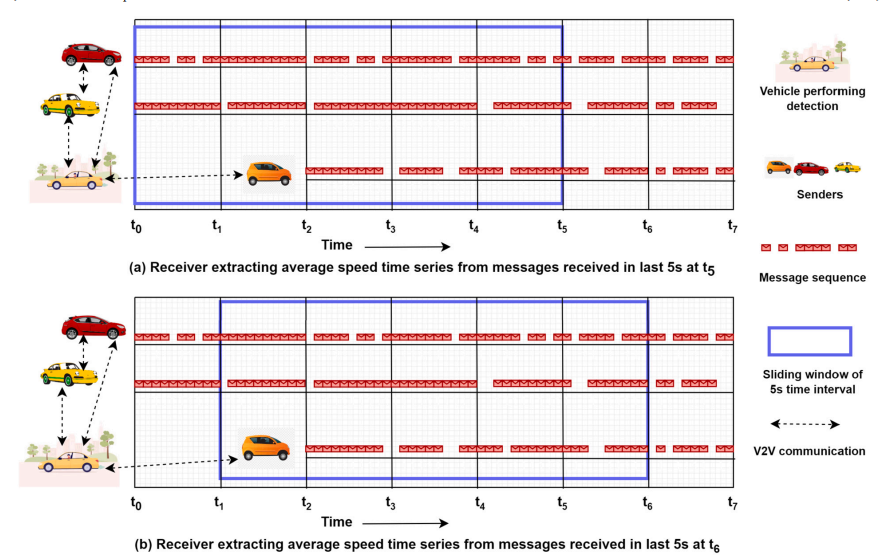
**Cooperative Data-Centric Detection** (DTW on speed series)

# Each vehicle exchanges data (average speed, density) with neighbors and updates its list every second. Using a hypothesis test, it checks if a sender’s speed is within the normal range. If not, the sender is marked **suspicious** and added to the suspicious node list.

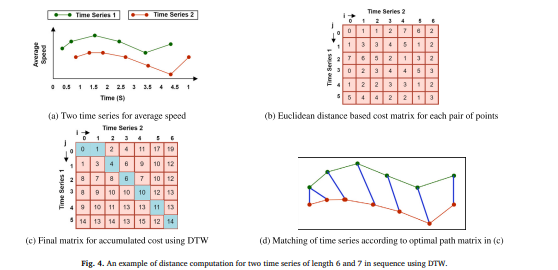
SUSPICIOUS NODE DETECTION

In this process, each vehicle checks its neighbors by comparing their average speed with the overall speed pattern of nearby vehicles. First, the vehicle calculates the **mean** and **standard deviation** of the average speeds received from its neighbors. If a neighbor’s speed falls within the acceptable range (mean ± standard deviation), it is considered **genuine**. Otherwise, the neighbor is flagged as **suspicious** and added to the suspicious node list for further verification.

# When a vehicle is marked suspicious, it is not immediately confirmed as a Sybil node. To verify or confirm , the system collects the past 5 seconds of average speed data for all suspicious vehicles and forms their time series. These series are then compared using Dynamic Time Warping (DTW), which can detect similarities even when the sequences differ in length or timing. If two or more suspicious nodes show highly similar speed patterns, they are confirmed as Sybil identities of the same attacker.



In the proposed method, the similarity between average speed time series is measured using DTW distance. Since Sybil identities come from the same attacker, their speed variations appear very similar, resulting in a low DTW distance. Instead of using a fixed threshold, the system adapts the threshold dynamically based on vehicle density, using Linear Discriminant Analysis (LDA). This ensures more accurate detection across different road and traffic conditions. Finally, if two nodes show both a low DTW distance and the same density value, they are confirmed as Sybil nodes belonging to the same attacker.



**Sybil detection method**

We confirm that nodes are **Sybil nodes** using two checks together:

1. **Similarity of speed behavior(DTW distance check):**
   * We calculate the Dynamic Time Warping (DTW) distance between the average speed time series of two suspected nodes.
   * If this distance is **very small (below the adaptive threshold Kᵥᵢ,ₜ)**, it means the two nodes are showing **almost identical speed patterns**.
   * This is a strong sign that they may not be independent vehicles, but identities controlled by the same attacker.
2. **Consistency of vehicle density (ρ check):**
   * We compare the **vehicle density value** reported by both suspected nodes.
   * If the density values are **exactly the same**, it suggests both nodes are being generated by the same attacker (since normal vehicles in slightly different positions would not have identical density readings).

* **Final Confirmation Rule:**  
  A pair of nodes is confirmed as **Sybil nodes from the same attacker** **only if** Their DTW distance is below the threshold, **and** Their density values match.
* **Node-Centric Detection** (DST at RSU)

**#** We need node-centric detection because local (vehicle-level) detection alone is not always reliable. A Sybil attacker may adjust its speed to stay within the normal range and avoid suspicion, or genuine vehicles may be wrongly flagged as suspicious. To overcome these issues, RSU-level verification ensures more accurate and trustworthy detection by combining multiple vehicle reports and reputation values. This helps confirm Sybil attacks, reduce false positives, and identify the actual malicious node more effectively.

In node-centric detection at the RSU, the limitations of local detection at vehicles—such as missing some Sybil nodes or falsely flagging genuine ones—are addressed through higher-level verification. The RSU collects detection reports from vehicles within its coverage area and applies Dempster-Shafer Theory (DST) to combine these reports for more reliable decision-making. Each vehicle is assigned a reputation value by the Certificate Authority (CA), which serves as supporting evidence in its reports. By combining detection evidence with reputation values, the RSU can confirm Sybil attacks more accurately while minimizing false alarms.

1. Vehicles Report (every second):  
   Each vehicle tells the RSU (roadside unit) which nodes look suspicious.
2. Make Pairs:  
   RSU looks at all suspicious nodes and forms pairs.  
   Example: Suspicious = A, B, C → pairs = (A,B), (A,C), (B,C).
3. Gather All Opinions:  
   For each pair, RSU gathers what all vehicles said about them.
4. Fuse Evidence (DST):  
   Using Dempster-Shafer Theory (DST), RSU combines these opinions into a single “belief score.”
   * bel(H): belief both are genuine.
   * bel(¬H): belief both are Sybil.

Decision rule:

* + If bel(H) > 0.5 → treat them as genuine.
  + If bel(¬H) > 0.5 → treat them as Sybil attackers.

1. Final Report & Reputation Update:
   * RSU sends its decision to the central Certification Authority (CA).
   * CA updates the reputation scores of all nodes (both reporters and suspects) using a Beta Distribution (like giving a probabilistic trust rating).

Example –

We have **2 suspicious nodes**: N1 and N2.  
Three vehicles (senders) give reports about them to the RSU.

| **Sender** | **Report on N1** | **Report on N2** |
| --- | --- | --- |
| V1 | Suspicious | Genuine |
| V2 | Suspicious | Suspicious |
| V3 | Genuine | Suspicious |

**Step 1: RSU Collects Reports**

RSU takes all the reports for the pair (N1, N2) from **all senders (V1, V2, V3)**.

**Step 2: Evidence Aggregation**

* N1 → 2 say *Suspicious* (V1, V2), 1 says *Genuine* (V3).
* N2 → 2 say *Suspicious* (V2, V3), 1 says *Genuine* (V1).

So RSU has a **combined belief** like this:

* N1: Suspicious (more evidence)
* N2: Suspicious (more evidence)

**Step 3: Apply Belief Threshold**

If belief > 0.5 (majority), then node = Suspicious (Sybil).  
If belief ≤ 0.5, then node = Genuine.

Here:

* N1 → Suspicious (2/3 > 0.5)
* N2 → Suspicious (2/3 > 0.5)

So, RSU decides: **Both are Sybil nodes**.

RSU doesn’t trust just one sender’s word. It **combines evidence from multiple vehicles** before deciding if nodes are genuine or Sybil.

**Key Techniques**

**DTW (Dynamic Time Warping): compares speed-time series to spot similarities between Sybil nodes**

Dynamic Time Warping (DTW) is a technique used to measure the similarity between two time series, even if they vary in speed or timing. In the context of VANET, DTW compares the speed–time patterns of vehicles. If multiple vehicles show highly similar speed patterns over time, it indicates that these nodes may not be genuine independent vehicles but Sybil identities controlled by the same attacker. This helps in linking suspicious nodes together and strengthening Sybil attack detection.

**DST (Dempster-Shafer Theory): aggregates suspicious + genuine reports at RSU**

DST is a **mathematical framework** that combines pieces of **uncertain or incomplete evidence** to produce a final **confidence level (belief)** about something.

Example:

* + RSU1 says: There is a 60% chance this vehicle is fake.
  + RSU2 says: There is a 70% chance this vehicle is fake.
  + DST combines these independent pieces of evidence → final belief might be 85% certain this is a Sybil node.

**Datasets:**

Simulates real attacks – By using the VeReMi dataset and increasing the message rate, it creates realistic scenarios of Sybil attacks in heavy traffic.

Tests detection methods – This setup allows the framework to check if it can correctly detect which vehicles are sending fake messages.

Handles different densities – By simulating high vehicle density and varying attacker numbers, it tests the system’s performance under challenging conditions.

Improves accuracy – Using realistic attack patterns helps the detection framework become more reliable in real-world scenarios.

**Conclusion:**

**Detection of connected Sybil nodes** – Most existing methods only detect the presence of Sybil attacks, but the proposed framework identifies which nodes are working together, helping trace the originating attacker.

**Combination of data-centric and node-centric approaches** – It uses cooperative detection (data-centric) and verifies reports at the RSU (node-centric), which improves accuracy and reduces false positives.

**Adaptive and lightweight mechanism** – The detection threshold adjusts dynamically based on the network context, making it efficient for real-time scenarios.

**Reduced overhead** – Compared to previous methods, it performs detection with lower computational and communication overhead.

**First framework of its type** – No previous work has simultaneously detected connected Sybil nodes and used node-centric verification while exploiting a few vehicle parameters.