
# Netaji Subhas University of Technology

## Opinion-Based Decentralised Malicious Intent Detection in Intelligent Transport Systems

**Prepared by: (Group 71)**
Pranav Kumar (2021UCA1910)
Rohan Kumar Mishra (2021UCA1919)
Chirag Rajput (2021UCA1921)

**Mentored by:**
Dr. Rashmi Chaudhry

**September 23, 2024**

# Table of Contents


| Section Title | Page |
|---|---|
| Introduction | 2 |
| Motivation | 3 |
| Literature Survey | 4 |
| Problem Statement | 7 |
| Objective | 7 |
| Methodology | 8 |
| Simulation | 13 |
| Future Work | 16 |
| References | 17 |

# Introduction

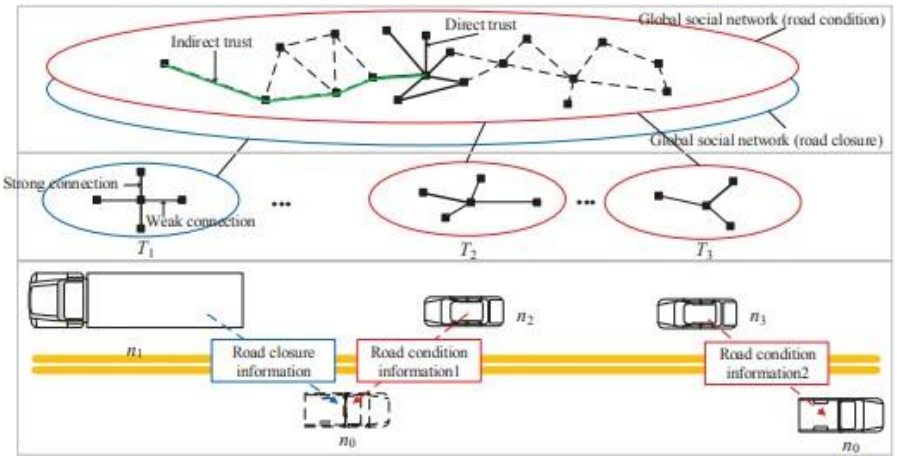
Emerging wireless technologies enable vehicles to connect to each other to form a vehicular network through wireless channels and share traffic- or entertainment-related information to provide improved safety and pleasure to drivers and passengers. Besides existing wireless technologies (e.g., Bluetooth), various connectivity solutions such as dedicated short range communication (DSRC), cellular network, and WiFi are being bundled with OEM manufactured cars. Potential applications of networking vehicles include enhanced driving safety, smart roadside information systems, and environment friendly transportation.

Various information are exchanged between cars in a vehicular network, including traffic jam, road constructions, incidents/crashes, road conditions and weather alerts, so it's important for a vehicle/driver to distinguish trustworthy from untrustworthy data. Vehicles sharing factual information with others are considered to be trustful, while those sending false information are distrustful. Currently, most research on trustworthy information sharing in vehicular networks rely on the public key infrastructure (PKI). Although PKI builds the first line of defense, it is possible for legitimate vehicles to send untrustworthy information due to defective sensors, computer viruses, and even for malicious reasons.

The communication is either V2V (Vehicle-to-Vehicle), V2I (Vehicle-to Infra) or hybrid via DSRC in a single or multi-hop mode.
Intelligent Transport System (ITS) ecosystem consist of vehicles with on board units (OBUs), roadside units (RSUs) set up along the roadways and a back-end system offering various services (registration, authorization, revocation). All these entities are interacting together for traffic control and improving road safety.

# Motivation

Car manufacturers have started equipping their vehicles with wireless access vehicular environment (WAVE) devices. WAVE protocols are based on IEEE 802.11p standard and provide basic radio standard for dedicated short-range communication. Every vehicle consists of an on-board unit (OBU), which broadcasts messages about its position, speed and other events. OBU has the capability to verify incoming messages from valid entities.




However, the dynamic and ephemeral nature of this network is also responsible for a wide variety of security vulnerabilities. Frequently disconnected network, vehicle density, high mobility and pattern of traffic flow are well-known challenges in ITS. These issues directly effect security protocols and safety on wheels. Due to high mobility nature, the network topology keeps on changing in a short span of time - strong medium access control (MAC) protocols are a prerequisite for effective data dissemination strategies to enhance throughput and reduce communication overhead.
A dynamic topology network is vulnerable to different security attacks.

Attacks like key/certificate replication, position faking and Sybil (malicious node create fake IDs and transmit false messages) are considered as critical attacks in ITS.
Confidentiality is also a security requirement in ITS, and it ensures the fact that data will only be read by an authorized entity.

Our motivation lies in making the network robust and secure to allow for an effective driving experience with increased fuel efficiency, shorter-time span travels and better traffic management.

# Literature Survey

We undertook a comprehensive survey of seminal works and pertinent literature in the realm of Vehicular Communications, IEEE Standard for Wireless Access in Vehicular Environments, Vehicular Social Networks(VSN), Cryptogrpahy and Blockchain. The knowledge gleaned from these works serves as the foundational bedrock upon which our research project is constructed.
Vehicular Networks are a special class of mobile ad-hoc network with predefined routes (roads). It relies on specific authorities for registration and management, Roadside units (RSUs) and On-Board units (OBUs). RSUs are widespread on the road edges to fulfill specific services and OBUs are installed in the vehicles navigating in VANET **[1]**.

VANETs are ad hoc networks, highly dynamic, with little access to the network infrastructure and offering multiple services. The communication modes in VANET can be categorized into Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Hybrid. In V2V, the used communication media is characterized by short latency and high transmission rate. [2]

This architecture is used in different scenarios of broadcasting alerts (emergency braking, collision, deceleration, etc.) or in a cooperative driving.

In the construction of a smart city, an intelligent transportation system (ITS) may be deemed to be the most crucial function given the proliferation of vehicles and the constant expansion of road networks [3].

5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC/WAVE, hereafter simply WAVE), as specified in a range of standards including those generated by the IEEE P1609 working group, enables V2V & V2I wireless communications. This connectivity makes possible a range of applications that rely on communications between road users and road operators, including vehicle safety, public service, commercial fleet management, tolling, and other operations [4].

One of the major challenges of securing ITS is communication security. This aims to provide secure communication between vehicles in ITS. Security is critical because a poorly designed ITS is vulnerable to network attacks, and this can compromise the safety of drivers.
There are numerous attacks that can disturb the security of the ITS and the privacy of its nodes (vehicles). The following are the most common devastating forms of attacks that an ITS can suffer [5]:

**Bogus Information**: Attackers can send wrong information in the network so that it can affect the behavior of other drivers.
**Alteration Attack**: This attack happens when attacker alters an existing data, it includes delaying the transmission of the information.
**Sybil Attack**: In this type of attack, the attacker uses different identities at the same time, these false identities also create an illusion that there are additional vehicles present.

**Denial of Service (DOS)**: Here, Attacker wants to bring down the network by sending unnecessary messages
**Tunneling**: The attacker connects two distant parts of the Ad hoc network using an extra communication channel as a tunnel. As a result, two distant nodes assume they are neighbors and send data using the tunnel.

Many researchers investigated the Trust evaluation within ITS [6-7] using various techniques. For the trust computation, it can be either based on the direct calculation for predefined parameters between two communicating vehicles (sender and receiver), or indirect calculation based on the neighboring opinion sent to the receiver about the sender for evaluation.

In this paper, we explore group-based architecture with hybrid opinion strategy that divides the entire network into sub-networks, based on radio-distance. Opinion about a vehicle transmitting event messages is calculated via direct as well as indirect measures to weigh-in the authenticity of the message passed.

Clustering can be used to improve routing scalability and reliability in VANETs, as it results in the distributed formation of hierarchical network structures by grouping vehicles together based on correlated spatial distribution and relative velocity [8].
In addition to the benefits to routing, these groups can serve as our foundations for implementing an opinion-based MID (Malicious Intent Detection).

# Problem Statement

Safeguarding and improving the security of Intelligent Transport Systems against various attacks that intend to cause harm to all drivers existing on the network, thereby improving driver safety, efficient travel and better traffic management.

# Objective

To develop a robust and scalable framework for enhancing the security and reliability of Intelligent Transportation Systems (ITS) by implementing an Opinion-based Decentralised Malicious Intent Detection. This framework will focus on:

- **Strengthening Communication Security:** Protecting vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications from common attacks, such as bogus information, alteration, Sybil attacks, denial of service, and tunneling.
- **Enhancing Trust Evaluation:** Utilizing decentralised hybrid opinion evaluation methods to assess the authenticity of messages transmitted between vehicles, thereby ensuring reliable information dissemination.
- **Exploring Blockchain:** Utilising blockchain for verifying the validity of the messages sent within a group to calculate Opinion about a vehicle in that sub-net
- **Promoting Safety and Efficiency:** Ultimately, to enhance driver safety, ensure efficient travel, and improve traffic management through a secure and reliable ITS framework.

# Methodology

For the problems presented above, we propose a Decentralised Opinion-Based Architecture using Blockchain.
This methodology describes the architecture and operational principles aimed at improving communication security and trust in Intelligent Transportation Systems (ITS). It is based on the framework provided by the National Highway Traffic Safety Administration (NHTSA), which categorizes its primary entities into four functional groups: policing, certificate processing, communication with vehicles, and misbehavior detection/revocation. This organized approach facilitates efficient management of vehicle interactions and the implementation of security protocols.
In our system, vehicles operate within groups facilitated by Group Representatives (GRs) and communicate with roadside units (RSUs) to relay information and updates to the backend system. RSUs act as base stations along roadways, employing Dedicated Short Range Communications (DSRC) protocols to enable seamless connectivity.

The architecture ensures that vehicles can report misbehaviors, receive certificate revocation lists (CRLs), and access critical traffic and safety updates. The optimal placement of RSUs is determined based on the road type—whether secondary roads or interstate highways—ensuring that communication remains robust across various environments.

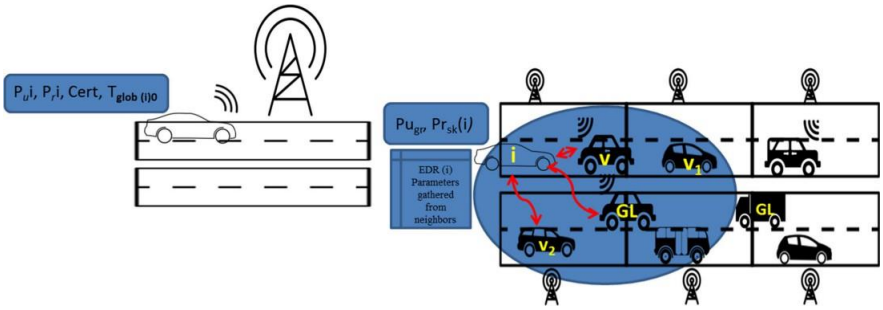
The opinion evaluation process plays a vital role in ensuring the integrity of vehicle communications. Each vehicle consistently monitors a variety of opinion metric parameters, which are classified into critical, intermediate, and optional categories. These parameters include factors such as communication quality, reliability of transmission and reception, GPS data, and sensor information. For example, when a vehicle joins a group, it starts broadcasting and receiving periodic beacons to and from its neighbors.

Each opinion metric is short-lived. This brief duration is essential in the fast-changing environment typical of ITS, enabling vehicles to swiftly adjust to alterations in their surroundings. By discarding outdated opinion metrics for vehicles that are no longer neighbors, the system reduces confusion and enhances the accuracy of vehicle behavior assessments.
The monitoring process is dynamic; as vehicles enter and exit specific areas, they constantly gather and update information about their surroundings, fostering a collaborative atmosphere for opinion evaluation across the network.

We employ an on-the-fly group formation model, which represents a dynamic schema. In this process, the Group Representative (GR) generates its own private key, the public key of the group, and the symmetric key for the group.
The private key is utilized to issue membership certificates to prospective group members, while the public key is used for identifying group members, and the symmetric key encrypts confidential data exchanged between group members, such as the opinion metric values of neighboring vehicles.

To enhance the security and transparency of key management, all keys and membership certificates can be recorded on a blockchain. This decentralized ledger ensures that any changes to group membership or key assignments are immutable and verifiable. Upon group formation, the GR broadcasts the keys for all vehicles within its group.
The details of this broadcast, including timestamps and the signatures, are then recorded on the blockchain to create a transparent history of group formation events.

When a vehicle requests to join a group, the GR verifies the new vehicle against the blockchain records to ensure it is legitimate. Once verified, the GR provides the new member with its secret signing key (group public key & group symmetric key).




Similarly, when a vehicle exits the group, the GR updates the group membership on the blockchain, ensuring that all authenticated members have access to the most current keys.

**Opinion-Formation Techniques:**

Each vehicle is initially assigned a global-opinion value of 0.5, implying that the vehicle is neither trustworthy nor malicious. Every vehicle ”forms” an opinion about other vehicles in its group, based on the periodic beacon messages transmitted by each vehicle (which contains, the position, velocity, GPS and other sensor data).
To form an opinion on the basis of all these parameters, we utilise geometric-mean of all values for a particular vehicle.

$O_{u,v}$ : Overall Opinion of Vehicle u about Vehicle v

$$O_{u,v} = [\prod_{i=1}^{k} \delta . m]^{1/k}$$

$\delta$ = *scaling factor*
$m$ = *opinion on ith metric*

This opinion metric will be used in future by other vehicles in the group to get a ”second-opinion” about the vehicle.

We propose a hybrid opinion approach that collects both the first hand and second hand opinion.

Second-Opinion about a vehicle is calculated by taking the arithmetic mean of all direct opinions about that vehicle of all the vehicles present in the group.

$SO_v$ : Second Opinion about Vehicle v

$$SO_V = \frac{1}{n}\sum_{i=1}^{n} O(i,v)$$

$O(i,v)$ = *Direct Opinion of Vehicle i about Vehicle v*
$n$ = *number of vehicles in a group*

Now the comprehensive opinion about a vehicle V by vehicle U is calculated as follows:

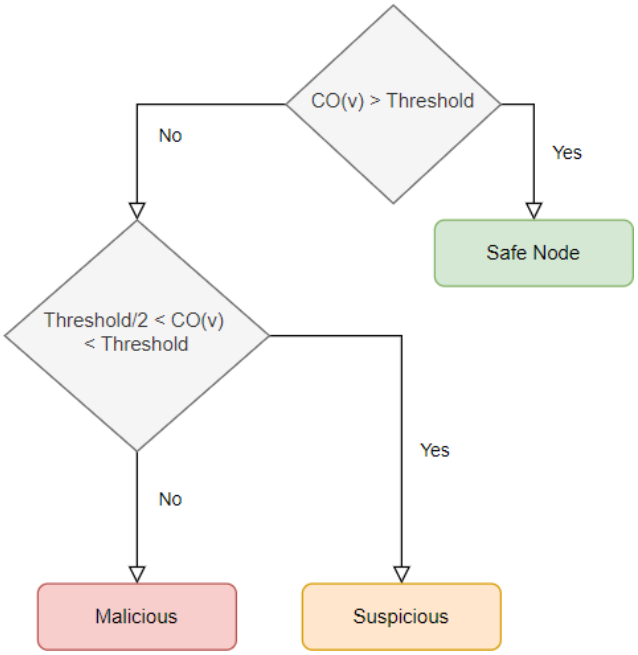
$CO_{u,v}$ : Comprehensive Opinion of Vehicle u about Vehicle v

$$CO_{u,V} = \alpha \,.\, O(u,v) + (1-\alpha).\ SO(v)$$

$\alpha$ = *scaling factor*
$\alpha \in [0,1]$

A malicious node is detected on the basis of this comprehensive opinion.

## Final Evaluation:



# Simulation Tools

### SUMO (Simulation of Urban MObility)

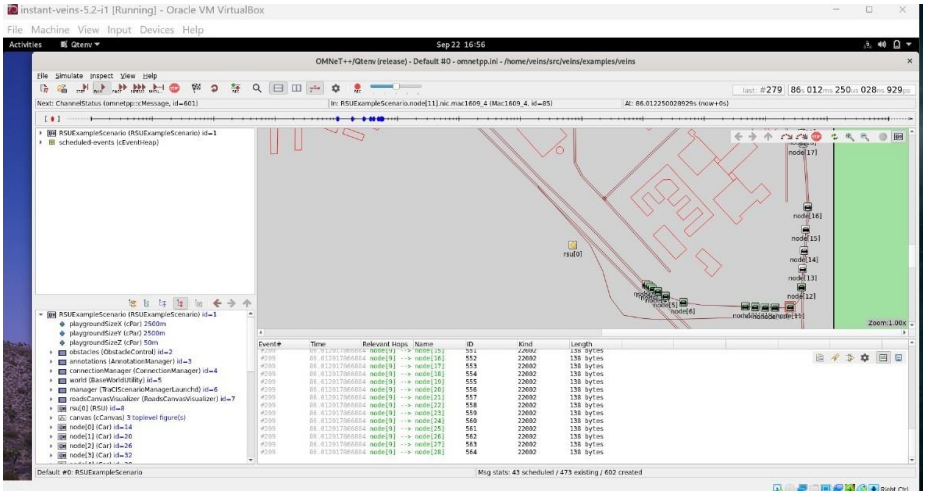
SUMO is an open-source, highly portable microscopic and continuous road traffic simulation package designed to handle large road networks. It allows for realistic modeling of traffic flows and behaviors, making it a valuable tool for traffic simulation.

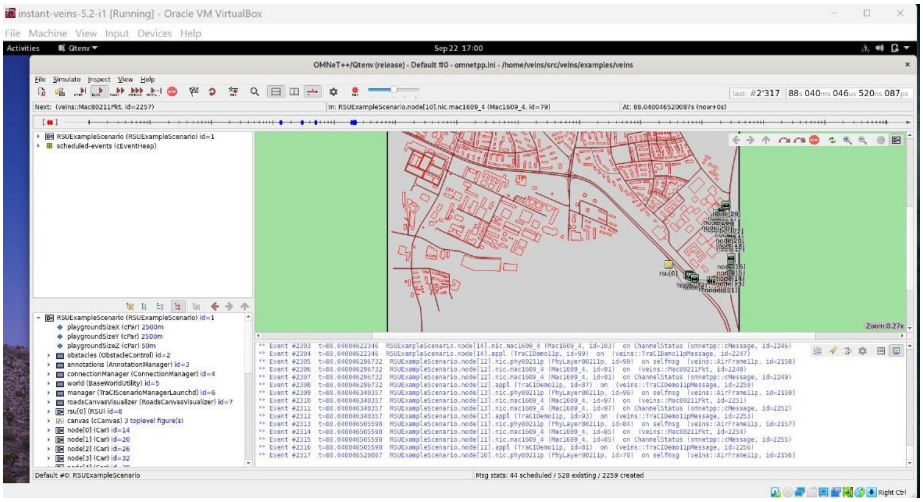
### OMNeT++

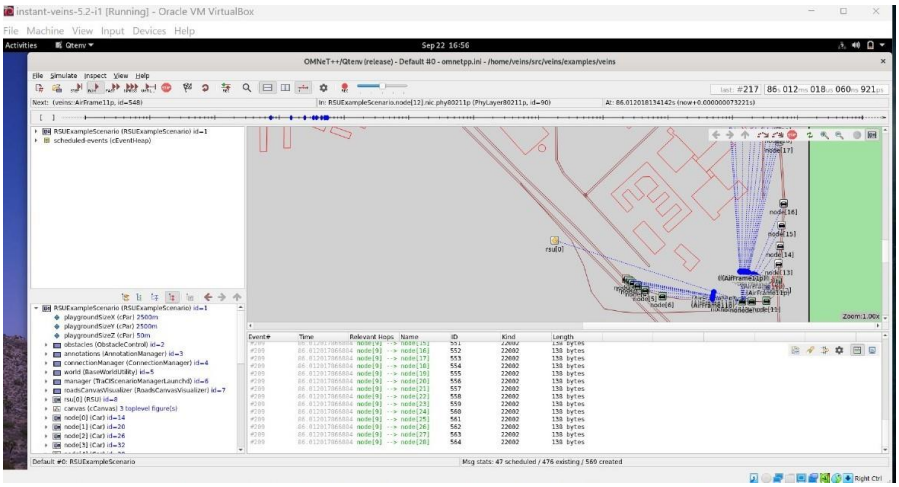
OMNeT++ is a versatile open-source discrete event simulation framework primarily used for simulating communication networks. The framework supports a broad range of simulations, including both wired and wireless networks, and is commonly used for research on network protocols and performance evaluation

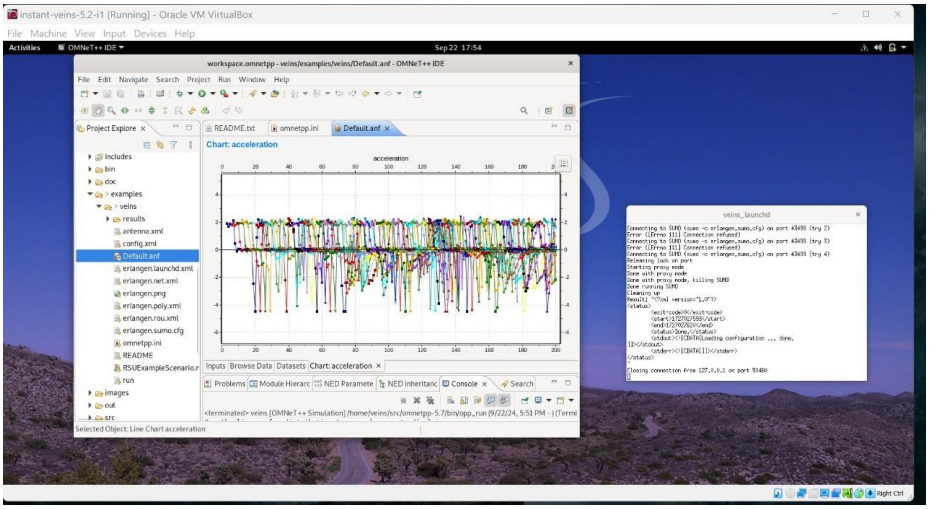
### Veins (Vehicles in Network Simulation)

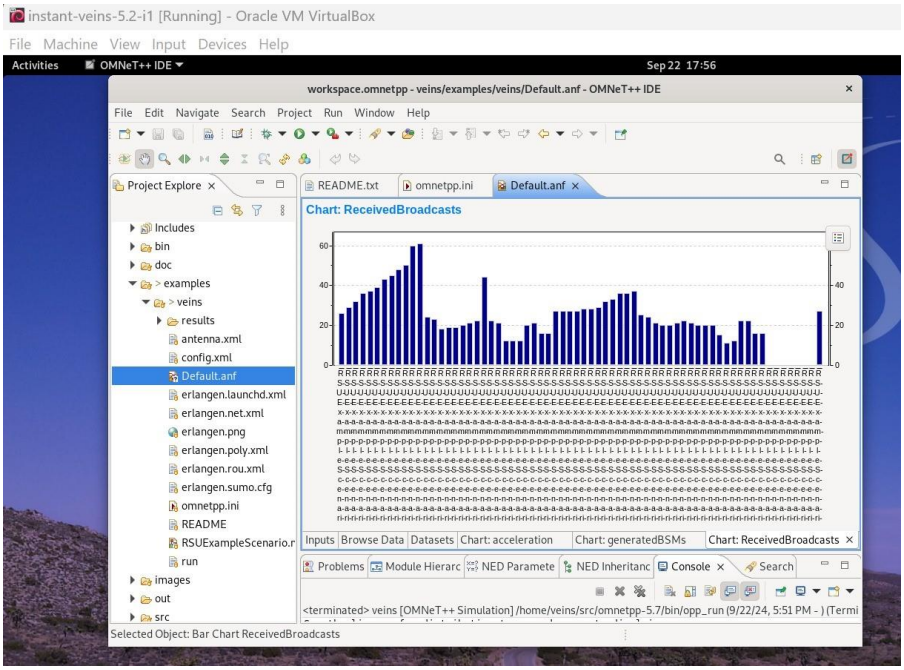
Veins is an open-source framework designed specifically for vehicular network simulations, integrating SUMO with OMNeT++. By combining the mobility models provided by SUMO with the network simulation capabilities of OMNeT++, Veins allows for detailed studies of vehicular networking. Its extensible architecture permits users to easily implement their own protocols and tailor traffic scenarios to their specific research needs.


instant-veins-5.2-i1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Qtenv
Sep 22 16:56
OMNeT++/Qtenv (release) - Default #0 - omnetpp.ini - /home/veins/src/veins/examples/veins
File Simulate Inspect View Help
Default #0: RSUExampleScenario


instant-veins-5.2-i1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Qtenv
Sep 22 17:00
OMNeT++/Qtenv (release) - Default #0 - omnetpp.ini - /home/veins/src/veins/examples/veins
File Simulate Inspect View Help
Default #0: RSUExampleScenario


instant-veins-5.2-i1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Qtenv
Sep 22 16:56
OMNeT++/Qtenv (release) - Default #0 - omnetpp.ini - /home/veins/src/veins/examples/veins
File Simulate Inspect View Help
Default #0: RSUExampleScenario




instant-veins-5.2-i1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
OMNeT++ IDE
Sep 22 17:56
workspace.omnetpp - veins/examples/veins/Default.anf - OMNeT++ IDE
File Edit Navigate Search Project Run Window Help
Project Explore
README.txt
omnetpp.ini
Default.anf
Chart: ReceivedBroadcasts
Includes
bin
doc
examples
veins
results
antenna.xml
config.xml
Default.anf
erlangen.launchd.xml
erlangen.net.xml
erlangen.png
erlangen.poly.xml
erlangen.rou.xml
erlangen.sumo.cfg
omnetpp.ini
README
RSUExampleScenario.r
run
images
out
src
Inputs
Browse Data
Datasets
Chart: acceleration
Chart: generatedBSMs
Chart: ReceivedBroadcasts
Problems
Module Hierarc
NED Paramete
NED Inheritanc
Console
Search
<terminated> veins [OMNeT++ Simulation] /home/veins/src/omnetpp-5.7/bin/opp_run (9/22/24, 5:51 PM - ) (Termi
Selected Object: Bar Chart ReceivedBroadcasts

# Future Works

We plan to explore fuzzy sets and machine learning techniques to figure out the best Comprehensive Opinion's Threshold values. Along with formation of opinion on a global level and not just within a group.

An important factor to keep in mind is the situation when the GR (Group Representative) itself exit the group due to range-exceed or unavailabilty. This situation calls for re-elections in the group to elect the next GR.
Another issue to be dealt with is related to selfish nature of nodes, rather than being malicious. Selfish nodes aim to utilise other nodes's resources while saving their own. As selfish behaviour doesn't last for a long time, detection of selfish nodes is challenging.

We plan to explore the scalability of our architecture as density of vehicles increase in an area. Movement of a vehicle across groups in a short span of time needs to be taken care of.
Utilising ML techniques for finding insights on the number of vehicles to be included in a group, based on a group's success rate to determine malicious nodes corresponding to the number of vehicles present.

# References


1. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANET security challenges and solutions: A survey. *Vehicular Communications*, 7, 7–20.

2. ETSI TS 102 940 V1.1.1- ITS—Communications security architecture and security management (2012).

3. Wang, J., Jiang, Ch., Zhang, K., et al. (2017). Vehicular sensing networks in a smart city: Principles, technologies and applications. *IEEE Wireless Communications*, 25(99), 1–11.

4. IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages: IEEE Std 1609.2-2016.

5. Tangade, Sh. S., & Manvi, S. S. (2013). A survey on attacks, security and trust management solutions in VANETs. In IEEE, 4th ICCCNT, Tiruchengode, India (pp. 1–6).

6. Patel, N., & Jhaveri, R. (2015). Trust based approaches for secure routing in VANET: A Survey. *Procedia Computer Science*, Elsevier, 45, 592–601.

7. Dixit, K., Pathak, P., & Gupta, S. (2016). A new technique for trust computation and routing in VANET. In Colossal Data Analysis and Networking (CDAN), Symposium on, IEEE (pp. 1–6).

8. Cooper, C., Franklin, D., Ros, M., et al. (2017). A comparative survey of VANET clustering techniques. *IEEE Communications Surveys & Tutorials*, 19(1), 657–681.