# Intrusion Detection in Vehicular Ad-hoc Networks (VANET) Using Post Processing Approaches

Saeed Jafari

8 November 2022

**Abstract**

The Vehicular Adhoc Network (VANET) is an integral component of Intelligent Transportation Systems (ITS) that facilitates communications between vehicles in order to improve safety and efficiency on the road. These networks can also be used by adversaries to spread false information. As a result, vehicles must be equipped with better cognitive capabilities as they relate to the data received. It is necessary to have intelligence and a means of evaluating the trustworthiness of the information received. Although VANETs are dynamic systems with connections and a lack of infrastructure, achieving this objective is very challenging due to their real-time constraints and connections.

Taking into account the potential peril, a model must be developed to detect nodes that feed false information to the vehicular network. The purpose of this research is to review and analyze approaches to detecting malicious nodes in VANETs. As another part of this presentation, we will present a novel supplementary method for identifying and isolating malicious entities by applying evidence theory to the pieces of information collected from all the network vehicles.

## Introduction

It has always been a challenge for human beings to use the fastest and safest vehicles. With 200,000 road fatalities occurring annually between 2000 and 2018, the need for a comprehensive approach to transportation security has doubled. It has been determined that there are several connections between the components of the transportation system. These connections can be classified into four categories: vehicle-to-vehicle communication (V2V), vehicle-to-pedestrian communication (V2P), vehicle-to-grid communication (V2G), and vehicle-to-infrastructure communication (V2I). A vehicle-to-vehicle communication system covers the blind spots of the driver and prevents collisions and traffic congestion. When the communication channels are not configured properly or attackers are able to interfere with the system, they may pose a potential threat to road safety. This could cause harm to human beings. Therefore, network designers must ensure that in the event of a technical failure or attack, the network will operate correctly.

There have been a number of studies conducted in this area focused on addressing the reliability of sending and delivering messages over VANETs. However, few have focused on measuring the validity of message content. Furthermore, authentication methods do not address this issue because of high mobility, rapidly changing network topology, limited bandwidth and processing power available, and privacy concerns associated with vehicles in these networks. Further, authentication methods cannot identify malicious entities that have been identified as illegible utilizing cryptographic algorithms. To ensure the validity of the content of VANET messages, a mechanism has been established to calculate the probability that VANET nodes are truthful. A mechanism called trust management prevents false messages in order to increase the security of VANET. Due to the incapacity of cryptographic-based approaches to deal with internal attackers, if one of the trusted nodes in VANET sends a fake message, it is not possible to detect that the message is not authentic. The overhead of cryptographic-based solutions is also unacceptable due to the distributed structure and dynamic topology.

## Brief Related Work

There are three types of trust management schemes: entity-based, data-oriented, and hybrid approaches. A data-oriented approach focuses on assessing the credibility of the data itself as opposed to entity-based approaches, which are concerned with measuring the trust level of a node. This approach is referred to as a hybrid scheme when it uses the reputation of nodes as a parameter for determining data trust. These types of trust management are used to categorize all studies in this domain.

## Technical Contributions

We will propose a malicious node detection module (MND) based on Bayesian Inference that detects node behavior in a centralized offline manner in order to stabilize the network by revoking nodes.