WEKA-based Real-Time Attack Detection for VANET Simulations

Yasmine CHAOUCHE
École nationale Supérieure d'Informatique
Algiers, Algeria
hy_chaouche@esi.dz

Éric RENAULT
ESIEE Paris
Paris, France
eric.renault@esiee.fr

Ryma BOUSSAHA
École nationale Supérieure d'Informatique
Algiers, Algeria
r_boussaha@esi.dz

***Abstract*—The number of connected vehicles has significantly increased in recent years and Vehicular Ad Hoc Networks (VANETs) are one of the most important technologies developed for these Intelligent Transportation Systems (ITS). In this infrastructure, vehicles continuously broadcast data to other vehicles and road side units (RSU) which leads to complex scenarios of connected vehicles. Moreover, due to their unique nature and characteristics, such as their high mobility, VANETs are highly vulnerable to various internal and external attacks. Our aim is to implement security measures, which includes the deployment of misbehavior detection frameworks to effectively mitigate these attacks.**

The Framework for Misbehavior Detection (F2MD) is one of the proposed solutions developed in this context. In this paper, we present an enhanced version of F2MD that utilizes the Waikato Environment for Knowledge Analysis (WEKA) for real-time detection of attacks in VANETs. Hence, we can leverage the wide range of algorithms provided by WEKA to perform real-time prediction and evaluation tests, conduct algorithm comparisons, and visualize the results. We validate our solution by comparing a set of selected algorithms available in WEKA. The Support Vector Machine (SVM) has been identified as the optimal choice in terms of prediction's speed and accuracy with a value approaching to 99%.

***Index Terms*—VANET, WEKA, Attack Detection, Real-Time**

I. Introduction

Intelligent Transport Systems (ITS) have been developed in order to improve the quality of citizens' lives, road safety and driving conditions. Vehicular Ad hoc NETwork (VANET) is a particular case of ad hoc networks and a technology developed in the context of smart ITS. It is counted among the most emerging subsets of the Mobile Ad hoc NETworks (MANET) [1] with a promising future and great challenges especially in cybersecurity.

The VANET is composed of nodes that communicate with each other and with the Road Side Infrastructure (RSU) through a communication unit installed in each vehicle named the On-Board Unit (OBU). In order to improve road safety and driving efficiency, this network provides timely exchange of information via Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication such as road condition warnings and emergency messages. However, security is one of the most critical issues in VANETs since these transmitted messages are distributed in an open access environment with high node mobility [2]. A malicious node can alter any information in the propagated packet and inject, delete, or transmit false messages. This can ultimately cause significant damage and safety issues on the road.

Today, machine learning is one of the most efficient artificial intelligence techniques that have been widely used to solve several problems such as attack detection. Many researchers have recently shown that integrating machine learning methods into Intrusion Detection Systems (IDS) increases their efficiency in detecting attacks [3]. The Waikato Environment for Knowledge Analysis (WEKA) [4] system provides more than 80 machine learning algorithms and models written in Java. It supports several standard data mining tasks such as data preprocessing, classification, visualization and feature selection. This tool allows a computer program to automatically analyze a large set of data and take the most relevant information. Therefore, this information can be used to automatically make decisions and predictions much faster and more accurately.

Simulators, such as VEINS [5], are useful and less expensive substitutes compared to the real implementation of VANETs which require high costs and intensive labor. In this type of vehicular network, they are used for several purposes such as the simulation of exchanges between nodes and the evaluation of attack or misbehavior detection (MBD) algorithms. F2MD [6] is one of the recent VEINS-based frameworks that has been developed. It represents a misbehavior detection framework built specifically for the cooperative intelligent transportation system. However, there are only some machine learning algorithms that have been implemented and used for evaluating the performance of several attacks injected in the system including LSTM and MLP [6].

We propose through this work a solution that seamlessly integrates WEKA into F2MD, enabling full, easy and effective use of the diverse machine learning algorithms provided by WEKA. Furthermore, our solution facilitates real-time detection evaluations, a novel contribution that, to the best of our knowledge, has not been explored in existing literature. Additionally, it facilitates model comparisons and result visualization, enhancing the overall effectiveness of the framework.

The rest of the paper is organized as follows: Section II describes related work, Sections III and IV present the F2MD framework and the datasets. In Section V, we present the proposed solution and explain how the WEKA models are called to make real-time predictions through this framework. Section VI shows the experimental setup and scenarios used