Accelerating Imperceptible Attack Detection in Smart Transportation: A Parallel Computing Approach

Hadi Rashid Hasan *, Mohsene Amjadian, and Amanj Khorramian
University of Kurdistan, Sanandaj, Kurdistan Province, 66177-15175, Iran
*Corresponding Author: Hadi Rashid Hasan, hadi.rashid@uok.ac.ir

https://doi.org/10.31972/iceit2024.065

Abstract

Intelligent transportation systems can improve the security, reliability and efficiency of urban transportation networks by using advanced technologies. These systems rely heavily on digital infrastructure as they are vulnerable to many types of cyberattacks. Including imperceptible cyberattacks which are a type of cyberattacks that occur periodically and are difficult to detect with traditional methods. The aim of this paper is to develop and apply advanced techniques to identify imperceptible cyberattacks using parallel computing. The objective is to improve the accuracy and efficiency of detection algorithms using parallel computing and to develop a robust framework capable of detecting and mitigating threats from undetected cyberattacks to the security and integrity of smart transportation systems.

Keywords: Cybersecurity, Imperceptible attacks, Intelligent Transportation Systems (ITS), Parallel computing, Threat detection.

1. Introduction

In recent years, there has been significant progress in vehicle transportation due to the integration of artificial intelligence in Intelligent Transportation Systems (ITS). By connecting vehicles with Vehicular Ad Hoc Networks (VANETs) and the Internet of Vehicles (IoV) paradigm, which enhances the capabilities of ITS, this new breakthrough has altered the way people and things move. Compared to traditional smart cities those using big data exhibit profound changes. A key component of smart cities is Intelligent Transportation Systems (ITS), which addresses major social issues like traffic congestion. Traditional road construction is limited by land and money, so ITS implementation is necessary to increase the road network's capacity. In order to establish links between automobiles and road networks, enable people, and enhance the regulation and control of transportation systems, it enables enhanced transport infrastructure and cutting-edge information technologies. The end product of this integration will be more effective, convenient, safe, and intelligent traffic management (Xiong et al., 2012).

The result of the evolution of the Internet of Things (IoT) has led to the proliferation of IoT devices, which has created a network where devices are constantly collecting data and transmitting it for automated analysis. This has led to the emergence of smart cities as comprehensive programs, such as smart transportation, smart manufacturing, smart grids, and smart buildings, which has gained popularity. Smart cities are based on data analytics and IoT infrastructure (Xiong et al., 2012). By incorporating advanced information and communication technologies into infrastructure and vehicles Intelligent Transportation Systems (ITS) seek to increase sustainability and safety.

In Smart Transport Systems By using advanced technology, urban transport networks can operate more securely, dependably and efficiently. This is because these systems are becoming more vulnerable to various cyberattacks due to their increased connectivity and reliance on digital infrastructure.

We need to acknowledge these risks and put strong security measures in place if we are to maintain the integrity and effectiveness of smart transport.

Numerous cyberattacks have damaged the efficacy and efficiency of these technologies, resulting in network failures. Imperceptible cyberattacks are one kind of cyberattack on smart transit. These assaults happen on a regular basis. These highly risky hacks target smart transportation networks by blocking certain streets to specific vehicles at specific times. These cyberattacks can be executed in two ways: either by altering the device code execution flow, or by obtaining console access to smart devices like RSUs and OBUs. In actuality, the attack is carried out as gently as possible to avoid detection. After then, everything goes back to how it was. Because of this, the attack is undetectable and challenging to find.

There are many difficulties in recognizing and developing countermeasures for these attacks, and the techniques for detecting them are no exception Thus far, research has generally followed this pattern: several detection approaches are offered, assessed, and analyzed after taking into account a cyberattack scenario. Typically these detection methods operate under the presumption that attacks occur continuously and have always been noticeable. It is difficult to identify these kinds of attacks with conventional techniques. It is challenging to ascertain whether an attack has taken place if the detection is not completed within the allotted time range. Because the attacker only targets a small number of vehicles within a predetermined time period in order to avoid being detected by the smart transportation system. Its intermittent nature makes assault detection challenging. These reasons suggest that in order to detect undetectable attacks, techniques other than conventional, predefined solutions are required. For identifying purposes in this study, the Street Density Framework approach is employed.

This study’s primary goal is to create and implement a cutting-edge method for detecting imperceptible cyberattacks using parallel computing. The objective of this work is to improve the accuracy and efficiency of the algorithm capable of identifying and mitigating the threats posed by invisible cyberattacks on the security and integrity of intelligent transportation systems through parallel computations and the construction of a resilient framework.

2. Literature Review

To manage and maintain the massive amount of smart connected objects and the massive amount of data generated these days requires an intelligent method. Therefore software-defined networking (SDN) is seen as a potential paradigm for Internet of Things (IoT) management. The Internet of Things (IoT) now permeates every aspect of our daily lives and significantly affects everything from how we drive to how we shop to what to eat and what not to eat to stay healthy. Due to the diversity of IoT applications, flexible, agile, and adaptive IoT architecture is required. Part of the design of an SDN-based Internet of Things architecture is to decouple the control plane from the data plane and integrate intelligent management features that aim to meet this requirement. The study (Bekri et al., 2020) that emphasis’s the efficiencies of IoT network management also investigates the relationship between SDN and IoT, with special emphasis on the part that SDN plays in enhancing the effectiveness of IoT network management. Also provided in that is a detailed analysis of SDN-IoT systems and applications. In addition, several unsolved problems and possible lines of research are listed.

Intelligent Transportation Systems (ITS) undoubtedly provide an opportunity for the sustainable growth of smart cities in the modern era. To reduce the number of hazardous materials released into the atmosphere Intelligent Transportation Systems (ITS) rely on advanced transportation technologies. Technology adoption is linked to smart mobility and ITS. The adoption of highly developed ITS is linked to a number of advantages, challenges, and obstacles. The most preferred alternative for sustainable urban transport systems, however, appears to be transportation, intelligent transportation systems, and smart mobility (as a part of a smart city). The challenges associated with ITS deployment in urban areas have been identified in a study (Tomaszewska, 2021) from the perspective of the urban transportation authority.

Intelligent transportation systems (ITS) are an important hallmark of smart cities. Congestion is currently a major social issue, and limits the cost and availability of land for conventional road construction. Therefore, to increase the capacity of the road network, ITS are essential. The government is investing heavily in further research and construction in order to ease the pressure on aging transport networks and make the most of the resources already available. Connections between vehicles, road networks and people can be strengthened based on improved transport infrastructure and advanced IT technologies. This will improve order and control of the transportation system by making the traffic management system more effective, convenient, safe, and intelligent (Xiong et al., 2012).

Intelligent Transport Systems (ITS) are one of the major steps towards vehicle automation in the growth of the road transport sector, which uses technology that enables vehicles to communicate with road infrastructure or each other. ITS can enhance traffic efficiency and road safety, by improving data quality and reliability, but only by guaranteeing data protection and cybersecurity. As a result of the increase in cyberattacks globally, especially in the area of transportation security, cybersecurity has gained more attention. Additionally, as the number of vehicles rises, the issue of traffic control becomes more pressing, particularly in intercity settings. A road traffic model and an urban transportation network model are offered in the study (Mfenjou et al., 2018). It also offers techniques for tracking traffic in intercity road transport networks and system modeling.

The government, business community, and academic community are paying close attention to ITSs as they prepare for the next wave of transportation. As a result of the prevalence and complexity of cyberattacks, worries about cyber security are also growing. Game theory has recently been applied to model and forecast the future actions of these sophisticated attacks. Study (Sedjelmaci et al., 2019) presents surveys on the application of game theory to defend ITS from assaults and weighs the benefits and drawbacks in terms of needed cost and security level.

The incorporation of cutting-edge technologies creates previously unheard-of opportunities and efficiencies as firms experience a swift digital revolution. But this paradigm change to a digitally driven world also brings with it a host of cybersecurity issues that need close scrutiny. Study (Farooq and Martin, 2023) examines how cybersecurity is changing in the age of digital transformation, highlighting major issues and developments brought about by a greater reliance on cloud computing, developing technologies, and networked systems. The research explores the various aspects of cybersecurity issues such as ransomware attacks data breaches, and vulnerabilities related to the Internet of Things (IoT).

Traffic lights were the first example of intelligent transportation systems (ITS) in use in 1868. Technology advancements have made it necessary to tackle transportation applications strategically while maintaining speed and environmental protection. For states, defending ITS infrastructure from cyberattacks has become a reputational concern. The provision of the requisite technology infrastructure is crucial for the cohesive functioning of the ITS systems, particularly those related to mapping communication, and geographic positioning. With the advancement of technology come risks, hazards, and cyberattacks, all of which should be avoided, particularly with regard to the systems that are being used. Research (Avcı and Koca, 2024) delves deeply into the ITS architecture, applications, communication technologies, and emerging trend technologies. It also contributes to the body of knowledge on ITS security and attacks prevention, including an analysis of the most significant cyberattacks that could affect ITS applications and the minimal security measures that can be implemented to protect ITS applications and infrastructures from these attacks.

Security researchers have shown how to compromise intelligent traffic lights to potentially cause traffic disruption and deteriorate public safety. While intelligent traffic lights are essential cyber-physical systems that help smart cities reduce road congestion and vehicle emissions, they also open a new frontier in cybersecurity. The goal of study (Li et al., 2016) is to raise public awareness of traffic light system cyber security vulnerabilities. To better understand and address security weaknesses, the paper offers a bi-level game-theoretic framework for evaluating traffic light systems cybersecurity risks.

Vehicle-based ad hoc networks have arisen as an intriguing, if difficult, field in which many novel applications might find a home. Even though this sector has been the subject of research over the past 20 years, large-scale practical implementation still takes time. This study (Rasheed et al., 2017) presents an overview of potential applications and existing obstacles for VANETs, including medium access control mechanisms, routing techniques, hardware and spectrum constraints, and security and privacy concerns.

Vehicle ad hoc networks (VANETs) are categorized as a type of mobile ad hoc network (MANET) application that can enhance traveler comfort and safety on the road. Researchers studying wireless and mobile communications have recently become interested in VANETs, which differ from MANETs in terms of architecture, problems, features, and applications. This study aims (Al-Sultan et al., 2014) to provide researchers and developers with a comprehensive understanding of VANET by outlining key features in one easy-to-read document. This eliminates the need to peruse multiple pertinent papers and articles, starting VANET protocols and applications.

Parallel computing applied in technologies such as bioinformatics and financial systems widely across domains offers promising solutions to these cybersecurity challenges. The study (Naeem et al., 2020) shows how parallel processing has revolutionized data analysis providing a model that can be adapted to ITS cybersecurity applications. In enhancing security measures within financial systems the role of parallel computing has been discussed in fraud detection and threat analysis emphasizing its potential applicability to ITS. For integration techniques such as those enabled by simulation tools such as SUMO and OMNeT++ parallel computing, practical applications in ITS are demonstrated. To help test and improve the cybersecurity framework. Show how these tools can effectively simulate complex network scenarios. However, combining these advanced computational techniques with existing ITS frameworks presents significant technical and logistical challenges.

3. Methodology

It is critical to recognize and lessen imperceptible cyberattacks since they pose a serious threat. Consequently, we employed the Street Density Framework method described in some former research studies (Amjadian and Khorramian, 2022a, Amjadian and Khorramian, 2022b, Amjadian and Khorramian, 2022c) to detect these attacks.

1. Street Density Detection

This framework operates by analyzing the density of vehicles on different streets over specified time intervals. A chart is generated, where the rows represent the streets, and the columns correspond to the percentage of vehicles present on each street during specific time slots. Each cell in this chart displays the number of vehicles on a particular street as a percentage relative to other streets at the same time.

Specifically, if the percentage of vehicles on a street during a given period is significantly lower or higher compared to other intervals, it suggests the possibility of an imperceptible cyberattacks aimed at disrupting traffic flow or compromising the safety and efficiency of the transportation system.

This significantly reduces processing time and enhances computational capacity, making it particularly effective in handling large and complex datasets, such as those generated by urban traffic systems.

The data is meticulously processed and validated to ensure accurate detection, enabling this framework to act as an early warning system that alerts experts to potential cyber threats. The proposed approach not only increases the robustness of intelligent transportation systems against imperceptible cyberattacks but also contributes to improving overall traffic safety and operational efficiency.

The framework has the following algorithm:

```
for each street $s_k$ in street do
    for each time slot $\Delta t_j$ in time_slots do
        vehicle_count ← count_vehicles_on_street($s_k, \Delta t_j$)
        total_vehicle_count ← count_total_vehicles ($\Delta t_j$)
        $D(s_k, \Delta t_j)$ ← vehicle_count/total_vehicle_count
    end for
end for
```

2. **Parallel Street Density Framework**

To address this challenge, we also implemented this approach in parallel, with the steps as follows:

```
Input: streets, time slots, num cores
Output: D - a 2D array
Initialize array D with zeros
Split streets into chunks based on num cores
parallel for each street chunk $S_{\text{chunk}}$ in streets do
    for each street $s_k$ in $S_{\text{chunk}}$ do
        for each time slot $\Delta t_j$ in time-slots do
            vehicle_count ← count_vehicles_on_street($s_k, \Delta t_j$)
            total_vehicle_count ← count_total_vehicles ($\Delta t_j$)
            $D(s_k, \Delta t_j)$ ← vehicle_count/total_vehicle_count
        end for
    end for
end parallel for
Join all threads
```

In order to carry out a smart transport scenario, software tools are required to create a map of the intended city, distribute the cars on the map, move them throughout the city, and communicate with other virtual sensors between the automobiles. These programs can better accomplish the objectives of the research if they are open source. Three simulators OMNeT++, SUMO, and Veins have been chosen to carry out this research in accordance with these needs.

OMNeT++

OMNeT++ is an extensible, modular, component-based C++ simulation library and framework primarily designed for building network simulators. Developed by Andras Varga at Budapest University of Technology, OMNeT++ serves as a discrete event simulation environment that models primary communication networks. The generic and scalable architecture extends its use to the simulation of complex IT models such as queuing systems and multiprocessor modeling (Tripp-Barba et al., 2019).

In our research on imperceptible cyberattacks on automotive networks, OMNeT++ played an important role in simulating different network scenarios and analyzing the impact of such attacks. This simulator bridges the gap between the open-source NS-2 simulator and the OPNET license-based simulator by offering free software with various features. It boasts a structure-based, modular, hierarchical and extensible architecture, making it very suitable for our simulation needs. Modules and components in OMNeT++ are built using the C++ language, and newer versions of the software program these modules through the C++ class library, which includes a simulation kernel.

We used OMNeT++ in conjunction with Veins, as an extension specifically designed for vehicle network simulation. Veins uses OMNeT++ to simulate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, and that work allows us to model and analyze the impact of cyberattacks on intelligent transportation systems (ITS). In addition to its powerful C++ foundation, OMNeT++ uses the Network Description Language (NED), a high-level language used to assemble individual components into larger modules and models. The simulation environment also features a graphical network editor (GNED), which includes a NED compiler, a command line interface (Cmdenv), a graphical interface (Tkenv), a graphical performance analysis tool (Plove) and a documentation tool.

Over the years to this end, researchers have developed many models and simulation systems for OMNeT++ across different fields. Most of these models are open source, created as independent projects, and follow their release cycles. The basic protocol model library of OMNeT++, known as the INET Framework, encompasses a wide array of models, protocols, and components for the Internet stack. The OMNeT++ team maintains the INET Architecture with contributions from the community, incorporating patches and new models submitted by users. INET serves as the foundation for many other simulation systems and is adapted for specialized applications such as vehicular networks (Veins, CoRE), overlay/peer-to-peer networks (OverSim), and LTE networks (SimuLTE). To investigate and detect accurate cyberattacks using the capabilities of OMNeT++ and its extensions, we were able to create a detailed simulation environment on vehicular networks. In order to analyze potential disruptions in traffic flow and ITS performance, which provided valuable insights against cyber threats to improve the resilience of such systems. The OMNeT++ simulation kernel, written in the standard C++ language, is compatible with any platform that supports a modern C++ compiler. The simulation IDE runs on Windows, Linux, or macOS (Varga, 2001).

SUMO

In order for VANET to have realistic results, we need to have a realistic map of vehicle movement such as in urban areas, weighted distribution of vehicles with specific traffic management behavior so that the simulations can depict close to a real environment. SUMO (Simulation of Urban Mobility) and is an open-source microscopy traffic tool used to generate vehicle movement patterns under a given footprint by manually creating or by importing road networks from OpenStreetMap, VISUM, and sumo on. Is now intensely engaged in VANET simulation due to its ability to. Support traffic management, multi-modal traffic, traffic lights, autonomous driving, vehicle connectivity, and so on. It also carries the Microscopy label, which means that each vehicle and its dynamics are modeled individually, making SUMO a distinctive choice among other motion simulators.

In the Veins framework, each vehicle in the SUMO simulation is represented as a compound module in OMNeT++. A manager module, acting as a TraCI client, connects to SUMO (the TraCI server) and subscribes to events such as vehicle creation and movement. Each node (vehicle) in OMNeT++ contains a mobility module, which Veins uses to advance the simulation at regular intervals, updating the node's mobility information (such as position, speed, and direction) based on the behavior of the vehicle described in OMNeT++ (Varga, 2001).

The arteries were developed under the MiXiM framework, which is used for simulation of radio wave propagation, interference estimation and signal strength utilization and wireless MAC protocols. These simulations are essential for enabling the physical and MAC layer of OMNeT++ (Krajzewicz, 2010).

In our research on detecting imperceptible cyberattacks on Internet of Vehicles (IoV) devices, we leverage Veins to simulate the impact of these attacks on Intelligent Transportation Systems (ITS). We can accurately model vehicle motion and network interactions by integrating SUMO and OMNeT++ in Veins providing us with a powerful platform to test and validate detection algorithms. We ensure that our simulations using Veins reflect real-world traffic patterns and network behavior, which leads to reliability and enhances the applicability of our research findings.

Veins

Veins is an integrated simulator specifically designed for Vehicle-Dedicated Networks (VANETs) as well as being open source. It combines the motion simulator SUMO (Urban Mobility Simulation) with the network simulator OMNeT++. Veins operates as an OMNeT++ project, integrating SUMO as its motion model to create a versatile simulation environment (Haidari and Yetgin, 2019).

Through a standard TCP communication protocol known as the Traffic Control Interface (TraCI) Veins facilitates the control and coordination of both OMNeT++ and SUMO. This protocol ensures that the vehicle motion in the SUMO simulation is reflected as accurately as the node motion in the OMNeT++ simulation.

Managing Natural Traffic Variations to Enhance Cyberattack Detection

The Street Density Detection Framework incorporates historical data to construct baseline traffic patterns, taking into consideration naturally varying traffic densities occurring during rush hours or special events. Through the analysis of historical traffic patterns, the framework detects common variations across time.

Clustering methods are subsequently used to categorise comparable traffic patterns, enabling the system to distinguish between anticipated fluctuations (such as those seen during peak loads) and atypical irregularities that could suggest cyberattacks.

This approach guarantees that the framework can adjust to different traffic conditions, therefore decreasing the likelihood of false alarms during times of heavy traffic while yet retaining its detectability to possible dangers. As a result, the system offers a robust and adaptable solution for detecting imperceptible cyberattacks in intelligent transportation systems.

4. Experimental Setup

The datasets used in this study for evaluating the performance of the street density algorithm designed for detecting imperceptible cyberattacks in Intelligent Transportation Systems (ITS) are outlined below.

Parallel Street Density Framework

- Name of the Dataset: Street Density Data.
- Source or Origin: Traffic management systems.
- Size of the Dataset: Includes data for hundreds of streets over multiple time slots.
- Types of Data Included: Numeric (percentage values representing vehicle density).
- Description: This dataset is organized into a diagram where rows correspond to streets and columns represent the percentage of vehicles on each street at specific time slots. This format helps determine the density of each street and identify any unusual patterns.
- Preprocessing Steps: Aggregating raw traffic data into percentages, normalizing the data across different time intervals, and validating the values to ensure accuracy.

For this, the simulators Veins (Vehicle in Network Simulator), OMNeT++ (Objective Modular Network Testbed), and SUMO (Simulation of Urban Mobility) have been employed. The parallelization of the algorithm has been implemented using the Python language. Python was chosen due to its strong library support for data management (Pandas, NumPy) and parallel processing (multiprocessing, threading, asyncio). The dynamic nature and rich library ecosystem of Python make it ideal for data-intensive parallel processing tasks **Table 1**.

Parallel programming model

To improve the efficiency of the street density framework the use of a parallel programming paradigm is essential by optimizing the processing of the data involved in our study and maintaining synchronization across multiple processors. This paradigm allows for the division of computationally intensive tasks, such as the assessment of vehicle density in many streets and time zones, into smaller, independent units that may be executed simultaneously.

By employing methods like data partitioning and utilizing tools like the Message Transfer Interface (MPI), we effectively disperse the computing workload among processors. This method greatly decreases the time it takes to execute and improves the system's capability to identify undetectable cyberattacks in real-time within the Intelligent Transportation System (ITS). As a result, the framework becomes more scalable and better prepared to handle massive amounts of data.

Evaluation of Performance without Data Splitting

The current study utilizes the entire dataset for evaluation without a dedicated split for training and testing. Although this approach offers an initial evaluation of the framework's performance, it does not comprehensively measure its resilience and capacity for generalisation. An imperative goal for future research is to partition the dataset into separate training and testing sections.

Implementing this approach would enable the training of the framework using a subset of the data followed by an assessment of its performance on previously unknown data. Such an evaluation would yield a more precise evaluation of its ability to detect novel hazards in practical scenarios. Further investigation of various data splitting methods, (such as k-fold cross-validation), and the analysis of the impact of different training set sizes on the framework's performance would improve our understanding of its robustness and ability to generalise. The successful use of this methodical evaluation process will improve the reliability of the framework and ensure its effectiveness in safeguarding intelligent transportation systems against imperceptible cyber threats.

Table 1. Simulation Parameters

Map	Erbil
Simulation Time	14400s
Number of Vehicles	959
Number of Traffic Lights	1
Network Protocol	OMNET++
Network Interface	802.11p
Vehicular Network Simulation Framework	Veins
Traffic Simulator	SUMO
Message Passing Interface	MPI
Algorithm implementation and parallelization	Python

5. Results and Discussion

In this section, the simulation results are analyzed. The city of Erbil whose map is shown in **Figure 1** was used for the simulation. In three different settings with 8, 16, and 24 time intervals, the simulation was run on all twenty-four of the city's streets (Amjadian and Khorramian, 2022b).

Figure 1. A Comprehensive Map of Erbil City, Iraq for Intelligent Transportation System Analysis

In this study, we used street density framework to detect imperceptible cyberattacks and parallelized those using Python. The algorithm is designed to analyze vehicle counts across various streets and time slots to identify potential anomalies indicative of cyberattacks.

To evaluate the performance improvement with parallel computing, we measured the execution time using different numbers of processor cores. The results are summarized as follows:

1. **Street Density Framework Results**

In order to execute and examine the parallel street density framework, we initially took the required data sets out of the simulator's output results.

The data extraction steps from the simulator are as follows:

1- Identification of streets: In the first step, all the streets in the city were identified and a unique identifier (ID) was assigned to each one.

2- Identification of vehicles: In the next step, the ID of all the vehicles moving in the simulator was extracted.

3- Entry time registration: The precise moment at which each car entered the simulator was documented in order to capture their motions during various time intervals.

This initial information is collected for both network states (without attack and with attack). After collecting the data, we need to thoroughly analyze it and create a new file that includes a comparison of the network in normal and attack scenarios. As a result, we created a detailed document that includes the vehicle density for each street at different time intervals.

In **Figure 2** you can observe the changes in each street over time, presented in the following format:

- X-axis (Time Interval): Displays the time periods, which could be in minutes, hours, or other units, depending on the data.
- Y-axis (Percentage Difference): Shows the percentage changes for each street, helping to understand how these changes vary over time.
- Colored Lines: Each line represents a specific street. Different colors and markers help in distinguishing between streets.
- Data Points: Indicate the actual values for each time interval.

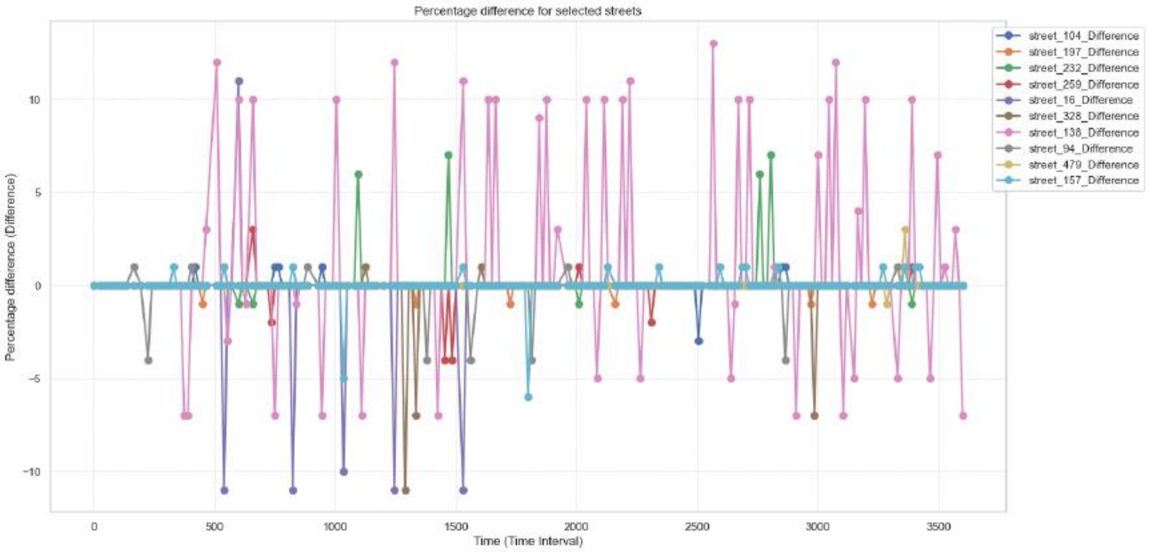

Figure 2. Percentage Difference Trends Across Selected Streets Over Time

A summary of the detection accuracy and false positive rate of our approach in detecting abnormalities and imperceptible cyberattacks is provided in the next section.

Accuracy Analysis and Performance Evaluation

To assess the effectiveness of the model the accuracy measure is computed using the following formula:

Definition: True positives (TP) are the number of correctly identified attacks.

The TN metric denotes the count of true negatives, which are correctly detected normal traffic.

False positives (FP) refer to the count of normal traffic that is mistakenly identified as an attempted attack.

False negatives (FN) can be defined as the count of attacks that are mistakenly identified as normal traffic.

The obtained values in our experimental results are as follows:

Total number of True Positives (TP): 36

Total number of True Negatives (TN) = 2

False Positives (FP) = 9

False Negatives (FN) = 0

Using these numbers, the accuracy of detection is computed as follows:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{36 + 2}{36 + 2 + 9 + 0} = \frac{38}{47} \approx 0.81 \; or \; 81\%$$

Based on the detection accuracy of 81%, our model demonstrates strong performance in accurately detecting most anomalies and cyberattacks. The attainment of an accuracy rate of 81% indicates that the model effectively identifies the majority of atypical variations in street density and undetectable cyber threats. The results exhibit the effectiveness and reliability of the suggested approach thereby enhancing security and operational efficiency in smart transportation systems.

False Positive Rate (FPR) Calculation:

To evaluate the performance of detection models, especially when detecting cyberattacks the false positive rate (FPR) is an important metric. FPR is defined as the proportion of normal traffic misclassified as a cyberattack. FPR is less indicative of a better performing model, which is essential to ensure the robustness and reliability of a security system.

The FPR is calculated using the following formula:

$$FPR = \frac{FP}{FP + TN}$$

Where:

FP (False Positives): The number of normal traffic instances that were incorrectly classified as cyberattacks.

TN (True Negatives): The number of normal traffic instances correctly classified as non-attacks.
In our study, the dataset contained 142,560 times with 26 instances predicted as possible cyberattacks. Of these nine cases were false positives, meaning they were misclassified as attacks. The total number of true attacks was 37, leaving 11 false negatives (i.e. undetected attacks).

$$FN = Total\ True\ Attacks - Total\ Predicted\ Attacks = 37 - 26 = 11$$

The total number of true negatives (TN) was calculated as follows:

$$TN = Total\ Slots - (FP + TP + FN) = 142560 - (9 + 26 + 11) = 142514$$

By applying the FPR formula:

$$FPR = \frac{FP}{FP + TN} = \frac{9}{142560 + 9} \approx 0.000063\ or\ 0.0063\%$$

This low FPR value of 0.0063% shows that our model has excellent performance in detecting ordinary traffic and imperceptible cyberattacks. A low FPR is a strong indicator of model reliability in real-world scenarios where decreasing false positives is critical to maintaining system operational efficiency.

These results demonstrate the reliability and effectiveness of our "Street Density Framework" approach in detecting imperceptible cyberattacks.

2. Evaluation of the Performance of the Street Density Algorithm in Multi-Core Configurations: A Comparative Analysis of Single-Core, Dual-Core, and Quad-Core Implementations

The findings of employing parallel computing to identify imperceptible cyberattacks using the street density algorithm are shown in this section. The **Table 2** indicates the outcomes we arrived at, which are as follows:

1. **Execution Time with 1 Core:** The execution time of the algorithm with 1 core is 13.28 seconds. This value represents the scenario where all operations are performed serially by a single core.

2. **Execution Time with 2 Cores:** When the number of cores is increased to 2, the execution time decreases to 12.12 seconds. This reduction reflects the performance improvement achieved through parallel processing, although the improvement is relatively modest. This could be due to the overhead of managing parallel processes or improper load balancing across the cores.

3. **Execution Time with 4 Cores:** When the number of cores is increased to 4, the execution time significantly drops to 7.91 seconds. This reduction indicates better utilization of parallel processing and load distribution across more cores.

Table 2. Parallel Computing Results for Detecting Imperceptible Cyberattacks

Parallel Street Density Framework	
Time taken with 1 cores	13.28 seconds
Time taken with 2 cores	12.12 seconds
Time taken with 4 cores	7.91 seconds

The parallel implementation of our algorithm has proven to be effective, demonstrating a substantial improvement in performance with the use of additional processor cores. These results highlight the potential of parallel computing to enhance the efficiency of algorithms designed for real-time detection of imperceptible cyberattacks in intelligent transportation systems. This improvement is crucial for ensuring timely and accurate detection, ultimately contributing to the robustness and reliability of intelligent transportation networks.

Utilizing efficient algorithms and leveraging parallel computing can improve the performance of detection systems, enhancing the security and stability of intelligent transportation networks.

The **Figure 3** reveals how the density of vehicles on specific streets changes over time. For example, in time slot 400, several streets exhibit a higher concentration of attacks (denoted by yellow points), suggesting these streets experienced unusual traffic patterns possibly due to an imperceptible cyberattacks.

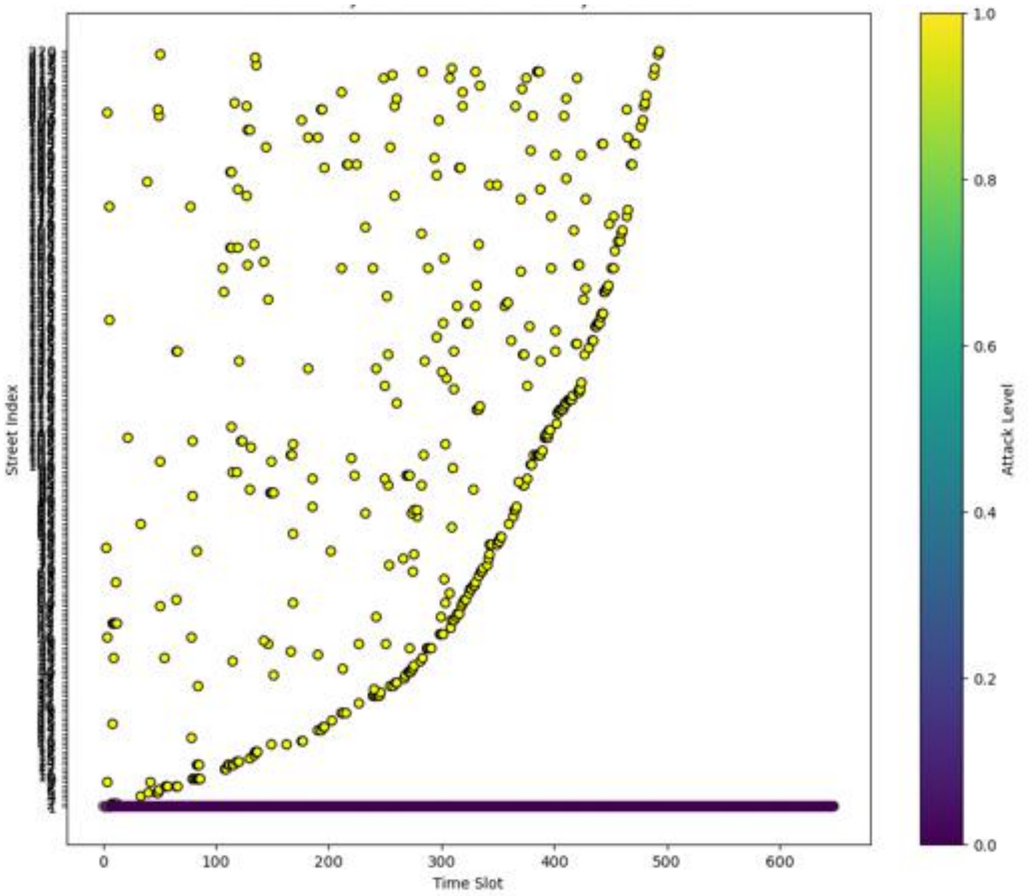

Figure 3. Detection of Imperceptible Cyberattacks: Parallel Street Density Framework Results

The **Figure 4** shows that increasing the number of cores can improve the execution time of the algorithm, but the reduction in time is not linear and may be influenced by factors such as communication overhead between cores and how the workload is distributed. However, using 4 cores has notably decreased the execution time, highlighting the benefits of parallel processing in such tasks.

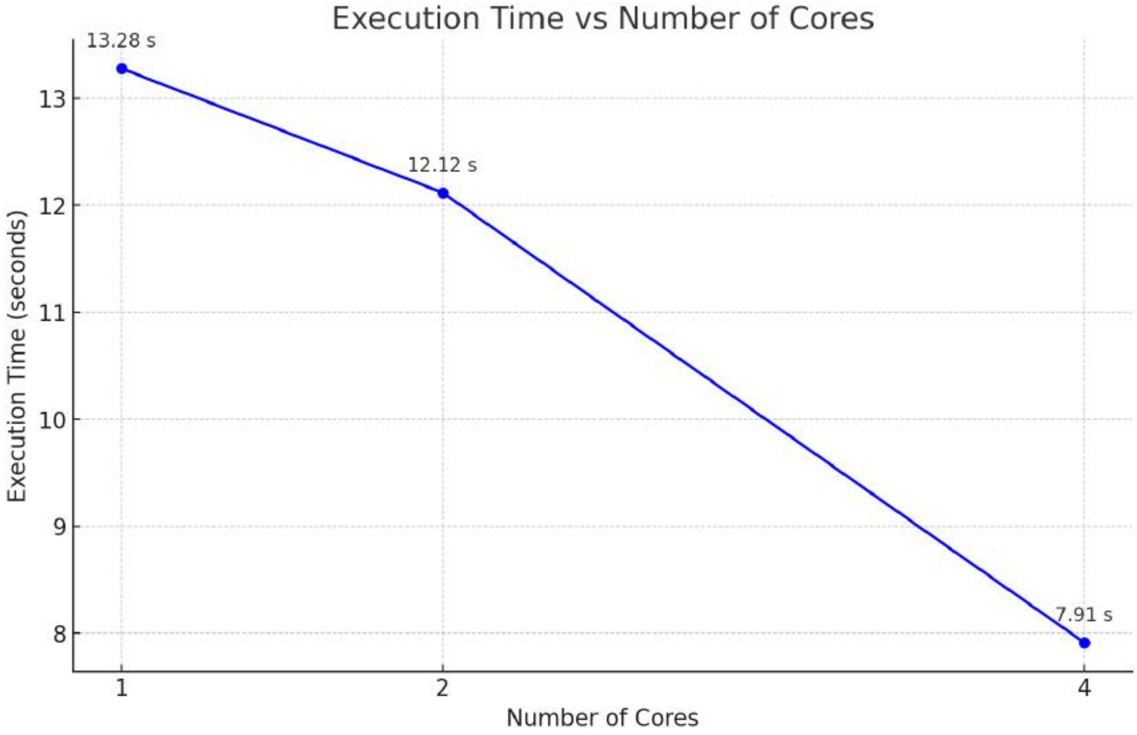

Figure 4. Impact of Core Count on Execution Time for Parallel Computing

To quantify this improvement, we calculated the speedup. It is calculated using the following formula:

$$Speedup = \frac{T_1}{T_n}$$

- T_1 is the execution time of the algorithm using 1 core (sequential execution).
- T_n is the execution time of the algorithm using n cores (parallel execution).

- T1=13.28 seconds (time with 1 core).
- T2=12.12 seconds (time with 2 cores).
- T4=7.91 seconds (time with 4 cores).

Speedup with 2 cores:

$$Speedup = \frac{13.28}{12.12} \approx 1.10$$

Speedup with 4 cores:

$$Speedup = \frac{13.28}{7.91} \approx 1.68$$

The speedup with 2 cores is about 1.10, meaning that using 2 cores provides a 10% performance improvement over 1 core.

The speedup with 4 cores is about 1.68, indicating that using 4 cores makes the algorithm approximately 68% faster compared to using just 1 core.

These speedup values indicate that the algorithm benefits from parallel processing, especially when using 4 cores.

6. Conclusion

In this research, we used the Street Density Framework method to identify imperceptible cyberattacks, implementing this detection approach in parallel. The parallel implementation of our algorithm demonstrated substantial performance improvement with additional processor cores, enhancing the efficiency of real-time detection algorithms. This improvement is crucial for ensuring timely and accurate detection, contributing to the robustness and reliability of intelligent transportation networks. Those with an interest in this area can conduct further experiments with larger datasets to understand the scalability limits of the algorithm and identify any potential bottlenecks. They can also develop a heuristic or dynamic approach to determine the optimal number of cores based on the dataset size. This would ensure that the computational resources are utilized efficiently.

7. Acknowledgements

We declare that no funding was received for conducting this study. Additionally, no contributors or institutions provided support for this research.

8. Conflict of Interest

The authors declare that there is no conflict of interest.

References

AL-SULTAN, S., AL-DOORI, M. M., AL-BAYATTI, A. H. & ZEDAN, H. 2014. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications,* 37**,** 380-392.

AMJADIAN, M. & KHORRAMIAN, A. 2022a. Detecting imperceptible cyber attacks and investigating its effects on the Total distances in smart cities (in Persian). *dcbdp2022*.

AMJADIAN, M. & KHORRAMIAN, A. 2022b. The impact of imperceptible cyber attacks on the traffic of the smart city of Songhor (in Persian). *University of Kurdistan*.

AMJADIAN, M. & KHORRAMIAN, A. 2022c. Impact of imperceptible cyber attacks on total time in smart cities (in Persian). *itctcnf.*

AVCı, İ. & KOCA, M. 2024. Intelligent Transportation System Technologies, Challenges and Security. *Applied Sciences,* 14**,** 4646.

BEKRI, W., JMAL, R. & CHAARI FOURATI, L. 2020. Internet of things management based on software defined networking: a survey. *International Journal of Wireless Information Networks,* 27**,** 385-410.

FAROOQ, O. & MARTIN, I. 2023. Cybersecurity Challenges in the Era of Digital Transformation. *Journal of Emerging Technology and Digital Transformation,* 2**,** 102-113.

HAIDARI, M. J. & YETGIN, Z. Veins based studies for vehicular ad hoc networks. 2019 International Artificial Intelligence and Data Processing Symposium (IDAP), 2019. IEEE, 1-7.

KRAJZEWICZ, D. 2010. Traffic simulation with SUMO–simulation of urban mobility. *Fundamentals of traffic simulation***,** 269-293.

LI, Z., JIN, D., HANNON, C., SHAHIDEHPOUR, M. & WANG, J. 2016. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. *IET Cyber-Physical Systems: Theory & Applications,* 1**,** 60-69.

MFENJOU, M. L., ARI, A. A. A., ABDOU, W. & SPIES, F. 2018. Methodology and trends for an intelligent transport system in developing countries. *Sustainable Computing: Informatics and Systems,* 19**,** 96-111.

NAEEM, M. A., JIA, X., SALEEM, M. A., AKBAR, W., HUSSAIN, A., NAZIR, S. & AHMAD, K. M. Vehicle to everything (V2X) communication protocol by using vehicular ad-hoc network. 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2020. IEEE, 384-388.

RASHEED, A., GILLANI, S., AJMAL, S. & QAYYUM, A. Vehicular ad hoc network (VANET): A survey, challenges, and applications. Vehicular Ad-Hoc Networks for Smart Cities: Second International Workshop, 2016, 2017. Springer, 39-51.

SEDJELMACI, H., HADJI, M. & ANSARI, N. 2019. Cyber security game for intelligent transportation systems. *IEEE Network,* 33**,** 216-222.

TOMASZEWSKA, E. J. 2021. Barriers related to the implementation of intelligent transport systems in cities-the Polish local government's perspective. *Engineering Management in Production and Services,* 13**,** 131-147.

TRIPP-BARBA, C., ZALDÍVAR-COLADO, A., URQUIZA-AGUIAR, L. & AGUILAR-CALDERÓN, J. A. 2019. Survey on routing protocols for vehicular ad hoc networks based on multimetrics. *Electronics,* 8**,** 1177.

VARGA, A. Discrete event simulation system. Proc. of the European Simulation Multiconference (ESM'2001), 2001.

XIONG, Z., SHENG, H., RONG, W. & COOPER, D. E. 2012. Intelligent transportation systems for smart cities: a progress review. *Science China Information Sciences,* 55**,** 2908-2914.