



# Article An Evidence Theoretic Approach for Traffic Signal Intrusion Detection

Abdullahi Chowdhury <sup>1</sup>, Gour Karmakar <sup>2,3</sup>, Joarder Kamruzzaman <sup>2,3</sup>, Rajkumar Das <sup>4</sup> and S. H. Shah Newaz <sup>5,6,\*</sup>

- <sup>1</sup> School of Computer and Mathematical Sciences, The University of Adelaide, Adelaide, SA 5005, Australia
- <sup>2</sup> Centre for Smart Analytics, Federation University Australia, Ballarat, VIC 3350, Australia
- <sup>3</sup> Institute of Innovation, Science and Sustainability, Federation University Australia,
- Ballarat, VIC 3350, Australia
   <sup>4</sup> Information Technology Services, Federation University Australia, Mount Helen Campus, Ballarat, VIC 3350, Australia
- <sup>5</sup> School of Computing and Informatics, Universiti Teknologi Brunei, Jalan Tungku Link, Gadong BE 1410, Brunei
- <sup>6</sup> KAIST Institute for Information Technology Convergence, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
- \* Correspondence: shah.newaz@utb.edu.bn; Tel.: +673-2461020 (ext. 5235)

Abstract: The increasing attacks on traffic signals worldwide indicate the importance of intrusion detection. The existing traffic signal Intrusion Detection Systems (IDSs) that rely on inputs from connected vehicles and image analysis techniques can only detect intrusions created by spoofed vehicles. However, these approaches fail to detect intrusion from attacks on in-road sensors, traffic controllers, and signals. In this paper, we proposed an IDS based on detecting anomalies associated with flow rate, phase time, and vehicle speed, which is a significant extension of our previous work using additional traffic parameters and statistical tools. We theoretically modelled our system using the Dempster–Shafer decision theory, considering the instantaneous observations of traffic parameters and their relevant historical normal traffic data. We also used Shannon's entropy to determine the uncertainty associated with the observations. To validate our work, we developed a simulation model based on the traffic simulator called SUMO using many real scenarios and the data recorded by the Victorian Transportation Authority, Australia. The scenarios for abnormal traffic conditions were generated considering attacks such as jamming, Sybil, and false data injection attacks. The results show that the overall detection accuracy of our proposed system is 79.3% with fewer false alarms.

Keywords: traffic signals; intrusion detection; intelligent transportation systems

## 1. Introduction

Traffic signals control traffic flows in different directions. This control reduces traffic jams and delays and bypasses incidents. Therefore, traffic signals are the heart of the city's traffic management of an intelligent transportation system. Intelligent transportation systems (ITSs) aim at making reliable, efficient, and protected transportation systems by integrating smart transportation management and control systems through communication networks and computing techniques [1]. Reliable and efficient traffic signals save lives by bypassing incidents and responding to emergency vehicles so that they can meet the target response time [2,3]. Traffic controllers control the traffic signals dynamically based on the traffic conditions derived from wirelessly collected sensor data. These sensors are installed in external places, such as being buried in the roads and equipped with roadside units. These sensors, their communication systems, and traffic signals are vulnerable to cyber attacks. Hackers or cybercriminals can easily create traffic disruptions or diversions by compromising the traffic signals to achieve the benefits they are interested in [4,5]. The chance of hacking or intruding traffic signals is sharply increasing over time because



Citation: Chowdhury, A.; Karmakar, G.; Kamruzzaman, J.; Das, R.; Newaz, S.H.S. An Evidence Theoretic Approach for Traffic Signal Intrusion Detection. *Sensors* **2023**, *23*, 4646. https://doi.org/10.3390/s23104646

Academic Editor: Han-Chieh Chao

Received: 28 February 2023 Revised: 26 April 2023 Accepted: 8 May 2023 Published: 10 May 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/). the signals are being equipped with more and more smart electronic devices and are increasingly dependent on wireless and internet-based data communications. The cyber security threats in the traffic signals will culminate at the peak when Autonomous Vehicles (AVs) hit the city's roads. AVs are a key component of an ITS. These AVs are equipped with advanced sensors and communication systems that allow them to operate without human intervention. Although there are many benefits of AVs, they are also vulnerable to cyber attacks because of their reliance on a range of connected devices and systems, such as GPS, sensors, and wireless communication networks. Hackers could potentially take control of an AV, causing it to malfunction or even crash [6–8].

The authors of [9] showed that disabling as few as seven signals in peak time periods for a couple of hours using a max vehicle affected model can cost around US USD 0.93 million, while the maximum vehicle flow targeting method can cost around US USD 0.98 million if 26 signals are impacted. The authors employed dynamic traffic assignment to show the consequences of traffic signal assaults and to mimic network-wide repercussions of intersection failures. The green traffic signal phase time analysis was also performed in [10]. It is imparted that the analysis of the patterns of green traffic signal phase time can be exploited to detect potential intrusion. However, in this study, a theoretical model for intrusion detection and its evaluation and validation were not specifically performed. In the current literature, there exist congestion-based attack analysis [11] and intrusion detection techniques [12] that exploit traffic image features. Additionally, with intrusion detection considering a specific attack, the other loopholes of these approaches rely on a selected set of traffic image features and an image prepossessing technique (background separation) that usually leads to being more computationally expensive. To advance the research in this area and introduce a more generic approach capable of detecting intrusion under various attacks, we introduced an approach for identifying traffic signal intrusion, which was published in [13]. However, the main problems of this approach are that important traffic signal parameter vehicle speed was not considered and mass value functions for flow rate and speed were not properly formulated. Additionally, there is uncertainty associated with probabilistic measures and converting the flow rate and vehicle speed data into normal distributions was not performed. By addressing these research issues, in this paper, we introduced a traffic signal Intrusion Detection System (IDS) with the following contributions:

- We developed a theoretical model for our proposed IDS, leveraging the Dempster– Shafer (DS) decision theory. Our model incorporates real-time observations of vehicle flow rate, vehicle speed, and traffic signal change duration, as well as relevant historical data obtained from transportation authorities. By utilising this decision theory, we sought to enhance the performance of our proposed system, leading to a more efficient and effective traffic control system. Our approach enables the integration of both historical and real-time data, facilitating the system's ability to make more precise and informed decisions.
- The historical data associated with traffic flow and vehicle speed were transformed into normal distributions. A heuristic mass function was introduced by assigning higher probabilities to those phase time values that are most frequently observed and are closer to the most observed value.
- To assess the uncertainty associated with our observations, we utilised Shannon's entropy. In order to verify and validate our proposed IDS, we developed a simulation model that is based on the SUMO traffic simulator [14]. Our simulation model incorporates real-world scenarios and utilises data collected by the Victorian Transportation Authority, Australia (VicRoads). The results of our simulations demonstrate that our proposed IDS is highly effective in detecting intrusions on traffic signals while reducing false alarms.

Since our proposed IDS is based on anomaly detection, it has the ability to detect intrusions created by the spoofed vehicles proposed in [11], as our method picks up any anomaly caused by intrusions, including intrusions in roadside sensors and traffic

controllers and signals. Flow rate, phase time, and vehicle speed are affected by the attacks in a traffic signal irrespective of their types. Therefore, in contrast to image analysis techniques, as mentioned before, our IDS is more generic because it detects by identifying the inconsistencies between the traffic flows, vehicle speeds, and phase time of the observed and normal traffic conditions. In summary, the overall advantages of our proposed solution are: (i) it is more generic and comprehensive in response to the intrusion of various forms, and (ii) it does not require any image capture and analysis as required by the above studies.

The organisation of the paper is as follows. Section 2 presents the related works on the impact of attacks on traffic signals and intrusion detection in traffic signals. Our proposed IDS along with its theoretical modelling is provided in Section 3. Finally, the experimental results and conclusions are given in Sections 4 and 5, respectively.

## 2. Related Works

To reduce traffic congestion and travel time, enhance traffic flow management, and protect the safety of road users, intelligent traffic systems, including traffic signals, are utilised [15]. Malicious disruption or manipulation of the lights of a traffic signal can result in catastrophic events such as massive delays, financial loss, and loss of life. Many traffic lights have recently been revealed to have been tampered with throughout the world, emphasising the necessity of precise intrusion detection. Since VANETs are important part of an ITS, a survey on machine learning based IDSs is presented in [16]. As VANET is an ad hoc vehicular network comprising vehicles and road side unites (RSUs), this survey did not consider IDSs for traffic signals.

Feng et al. [6] indicated that intruders could send malicious, spoofed, and corrupted data to the traffic signal control units. These exposures exhibit the pressing need to develop an intrusion detection system for traffic signals. So far, some research studies exist for assessing the impact of attacks on and detecting intrusions in traffic signals. These studies are presented in the following sections.

### 2.1. Intrusion in Traffic Signals

Intrusion attacks in intelligent traffic signals can cause significant safety hazards and traffic disruptions. Intrusion in traffic signals and traffic control systems refers to any unauthorised access, attack, or disruption of the system's functionality, which can compromise the safety, privacy, and security of the system and its users. Intelligent transportation systems use advanced technology and communication networks to optimise traffic flow, reduce congestion, enhance safety, and improve overall transportation efficiency. These systems rely heavily on connected devices, sensors, data processing, and communication networks, making them vulnerable to cyber threats.

Intrusion threats in intelligent traffic signals can be launched by intruders from outside the network using various methods. Some common intrusion attacks include replay attacks, jamming attacks, Sybil attacks, and false data injection attacks. A jamming attack is an intrusion attack in which an attacker sends messages to a specific RSU, disrupting the communication between the targeted RSU and other RSUs in the network. This can prevent the RSU from receiving essential messages or updates, leading to potential safety hazards or traffic disruptions. Replay attacks intercept the messages exchanged between sensors in the ITS network and re-transmit them to impersonate and steal their identity. This can allow an attacker to gain unauthorised access to the network or impersonate a legitimate user, potentially leading to data theft or other malicious activities. Sybil attacks are another type of intrusion attack where an attacker uses multiple identities to deceive other sensors by reporting fake road congestion. By flooding the network with false information, the attacker can disrupt traffic flow or cause congestion in specific areas, leading to potential safety hazards or traffic disruptions. False data injection is another type of intrusion attack, where an attacker sends false information about the current traffic situation on the road. This can lead to traffic disruptions or congestion, potentially causing safety hazards or delays for drivers.

A ransomware attack hit San Francisco's Municipal Transportation Agency in November 2016, preventing the agency from collecting fares and leading to several key systems shutting down. The attackers demanded a ransom payment of 100 Bitcoin (around USD 73,000 at the time) to restore the systems [17].

The city of St. Louis' traffic system was hacked, causing the city's traffic lights to go dark for several hours. The attack disrupted traffic and caused several accidents, highlighting the potential danger of hacking into critical ITS infrastructure [18].

Implementing robust security measures to prevent unauthorised access and manipulation is important, including access controls, encryption, network segmentation, and ongoing monitoring and testing of their systems to identify and address vulnerabilities.

### 2.2. Evaluating the Impact of an Attack on Traffic Signals

The U.S. Department of Transportation (USDoT) uses the Intelligent Traffic Signal System (I-SIG) to increase traffic management efficiency, reduce traffic congestion, and increase safety [19]. An approach presented in [20] to perform a data spoofing attack on I-SIG demonstrated that the data spoofing could be highly effective in manipulating the signal control algorithm. The spoofed trajectory analysis of the study shows that one single attack could increase the traffic delay by up to 68.1%. Introducing I-SIG improves traffic mobility by 26.6%, but only a single attack can make the traffic condition 23.4% worse than the traffic condition without using I-SIG [21]. Anomalies in traffic control systems not only increase traffic congestion but can also contribute to substantial financial loss. An intruder was able to attack the security cameras used in the Carmel Tunnels toll on a major road network in Haifa, Israel, on 8 September 2013. This cyber attack caused around eight hours of disruption, created enormous logistic issues, and cost hundreds of thousands of dollars [22].

### 2.3. Detecting Intrusions in Traffic Signal

Traffic congestion is considered a severe challenge to urban areas as it harms economic growth, increases gas emissions, and may lead to increased numbers of accidents [23]. Therefore, intelligent traffic signal management is crucial. The algorithms governing intelligent traffic signals are vulnerable to connected vehicle data spoofing attacks, resulting in the creation of congestion at road intersections. To overcome this problem, the foremost important step would be timely and accurate congestion attack detection and identification.

Xiang et al. [11] applied empirical studies to detecting intrusions in traffic signals. From a range of traffic images (vulnerable to potential data spoofing attacks), the solution measures the traffic flow characteristics and predicts whether there would be any attacks that would be able to cause congestion with a certain probability. Additionally, to verify any congestion occurrence, the authors proposed a tree-regularised gated recurrent unitbased approach that analyses the underlying relation between the congestion attack and traffic flow features at a given time. Therefore, when there is an attack that may lead to congestion with high probability, as well as if any congestion development is observed from the subsequent traffic flows, a congestion attack can be inferred. Based on an experiment, the authors imparted that the solution performs well in terms of attack detection accuracy and timeliness. They also proposed to validate their prediction by using traffic parameters in an intersection to determine if congestion really occurs as a result of placing spoofed vehicles in the intersection. Although this model can detect intrusion created by spoofed vehicles, it cannot detect intrusion created by malicious users modifying the data through unauthorised access to the traffic controller unit. This scenario will create congestion in intersections without having any indication from the image generation model.

The authors of [24] highlighted that the existing solutions for identifying congestion attacks have the disadvantage of delay. Considering that a congestion attack is made continuously and periodically, the authors developed a solution for predicting congestion attacks and attack frequency and the timely forecast of future congestion attacks. The prediction mechanism uses supervised machine learning algorithms where historical data are fed in. The solution collects traffic flows of variable spoofing frequencies and, then, the flows that lead to congestion are used to extract important features. It implements ensemble learning to establish correlations between various traffic flow features and abnormal congestion and attack frequency. The authors demonstrated the significance of their solution based on experimental results.

Li et al. [12] introduced a traffic image feature-based attack prediction mechanism. They claimed that, based on feature-based learning, it is possible to understand the relationship between attack and the caused congestion. Using a cycle generative adversarial network, the authors proposed a prediction mechanism where L1 regularisation loss is made to understand and recognise the difference between the last-vehicle and the firstvehicle attack.

Even though the image analysis technique was adopted as a universal technique for road safety, the 5th-generation adaptive traffic signal management system [25] employs self-learning capabilities and real-time computations to enhance the quality of traffic management for both conventional and autonomous vehicles by observing real-time traffic situations using different in-road sensors and RSUs. The traffic management system can independently learn traffic management strategies and make wise choices to optimise traffic flow, reducing the computational decision-making load incurred by image analysis techniques.

Most Adaptive Traffic Systems (ATSs), such as SCATS [26], SCOOT [27], and OPAC [27], use sensors to count vehicles and pedestrians and monitor vehicle speed. These ATSs use vehicle count sensor data, average vehicle speed data, and cell arrival and departure data. Most traffic signal intrusions occur by compromising roadside sensors [28]. So, it is crucial to develop a traffic signals intrusion detection system that utilises data collected from roadside sensors rather than relying on image analysis techniques. Other inherent issues associated with image analysis techniques are selecting optimised feature sets and separating background images, further contributing to its high computational requirements.

The framework developed by the authors of [10] allows for the identification of potential attacks on traffic control systems through the use of visual analytics and data collected from traffic signals. This framework provides a comprehensive overview of traffic signal data by breaking down traffic light cycles and calculating statistics on their duration and distribution over a given time period. By normalising individual traffic light cycles, the framework can detect potential abnormal patterns, making it possible to differentiate normal from abnormal traffic signal behaviour. This method of analysis can be an effective tool for identifying and mitigating potential security threats to traffic control systems.

The paper [13] describes our initial work on detecting intrusions in traffic signals by analysing vehicle flow rate and phase time at intersections. The DS decision theory was used to combine the evidential observations of these two traffic characteristics, using historical data provided by the Victorian Transportation Authority in Australia (VicRoads) and the SUMO traffic simulator to simulate intruded and typical traffic scenarios. We evaluated the performance of the proposed IDS under both normal traffic conditions and induced intrusions.

However, the intrusion detection approach described in [13] has some limitations. Firstly, it does not consider vehicle speed, which is an important traffic characteristic. Moreover, the mass value function defined for flow rate and phase time is not adequately specified, since the minimum value of the mass function is set to 0.5, whereas in reality, the mass function values should range from 0 to 1. Additionally, it does not address the uncertainty associated with the signals being normal or abnormal. This paper focused specifically on addressing these practical research issues to improve the accuracy and effectiveness of intrusion detection in traffic signals.

### 3. Proposed Intrusion Detection System

Anomaly-based intrusion detection can be particularly effective for detecting new or unknown threats that may not be detected by signature-based intrusion detection methods,

which rely on known patterns or signatures of known threats. Anomaly-based detection is useful because it can detect previously unknown attacks and it does not require prior knowledge of the attack signature. For detecting an intrusion in an intelligent traffic signal, these merits motivated us to propose an anomaly-based intrusion detection system in this paper. This system involves creating a baseline of normal traffic patterns and behaviour using historical traffic data and then monitoring the traffic for any deviations from this baseline that indicates a potential intrusion.

The implementation of anomaly-based intrusion detection for intelligent traffic systems involves several steps:

- Data collection: Traffic data are collected from the intelligent traffic system, including information on traffic flow rate, vehicle speed, and phase time.
- Baseline generation: A baseline is generated from the collected traffic data, which represents the normal traffic patterns and behaviour for the system.
- Anomaly detection: The traffic data are continuously monitored for any deviations from the baseline. Significant deviation from the baseline is flagged as potential anomalies and investigated further.
- Response: Once an anomaly is detected, the system sends an alarm to the traffic controller.

Details of our proposed model are given below.

### 3.1. Overview of the Proposed IDS

Our proposed system primarily monitors the state of a current traffic light, which is statistically calculated based on the flow rate, vehicle speed, and the traffic signal's phase time. The current state of the traffic signal is compared and contrasted with the relevant status of the traffic signals obtained from the related historical data collected by its Traffic Management System (TMS) [29] infrastructure to determine if it is functioning normally or abnormally. The operational flow chart of the proposed IDS is depicted in Figure 1. There are seven steps in our proposed intrusion detection system. The intrusion detection process starts in Step 1. In Step 2, our system collects data on road traffic, including flow rate, average vehicle speeds, and phase time. The details of the simulation used for the data collection are given in Section 4.1. In the third step, the mass values in probabilistic terms for each traffic condition (flow rate, vehicle speed, and phase time) are calculated. Sections 3.3–3.5 describe the details of this step. The mass values are then fused to find the belief value of the normal traffic condition in the fourth step. In the next step, the system checks if the fused value equals or exceeds the threshold value (defined in Section 4). If the value is above the threshold value, the traffic condition is determined to be normal and the system continues observing the traffic data. If the value is below the threshold, our system goes to Step 6 and sends an intrusion detection alarm to the traffic controller. Step 7 ends the intrusion detection process.



Figure 1. The operational flow chart of the proposed IDS.

# 3.2. Monitoring the Status of the Traffic Signal

Our suggested technique starts the intrusion detection assessment process in the second step by using a historical traffic pattern probability mass function that has not been tampered with by an intruder at a certain moment inside a specific time window (e.g., from 08:00 a.m. to 09:00 a.m. on Monday).

We acquired all relevant data from VicRoad's traffic data [30] for this research because we wanted to use previous data to monitor the state of a current traffic light at a certain moment. After this, we go through how to estimate the probability mass function of these data for a certain time window.

In the second phase, we need to calculate the continuous observed values of the traffic signal attributes for intrusion detection. We selected the three most important traffic attributes, namely traffic flow rate, signal phase time, and average vehicle speed. Attackers can change the phase time information manually and/or change the phase time by changing the flow rate information in an intersection and/or modify the average vehicle speed to falsify the traffic data. For example, hackers can extend the signal phase time to create disruption for plotting terrorist activity or a thief can extend a green signal phase time to pass quickly by a stolen vehicle. Vehicle speed was selected as it is also profoundly affected by traffic signal disruption. The impact of their changes only stays for one or two cycles, not being sufficient to create considerable disruption.

To determine whether a traffic signal is functioning normally or abnormally, we employed an inference method based on DS decision theory [31]. This theory, which is an extension of Bayesian theory, provides distributed support for various propositions based on temporal evidence. Our system defines the frame of discernment using three propositions: N,  $\neg N$ , and ( $N \lor \neg N$ ), which represent the current observation being normal, not normal, and uncertain, respectively.

Since flow rate, vehicle speed, and phase time are measured by individual sensors, the belief function contributing to each proposition must be statistically measured for each sensor. Let  $R_{jw}$  denote the id of a sensor located at intersection *j* with sensor type *w*, where  $w \in F, S, P$  represents the observed events of flow rate, vehicle speed, and phase time, respectively. As these events are observed over a time period for a given intersection, we utilised probability mass functions based on historical data from the corresponding time window of that day to determine the probability of a particular observation is normal. These time windows may differ for working and non-working days and are typically one hour in duration (e.g., 08:00 a.m. to 09:00 a.m. or 09:00 a.m. to 10:00 a.m.). The lower limit of the probabilistic value of *j*<sup>th</sup> intersection being normal for *y* events can be defined using the belief function of the DS theory [32]:

$$bel_j(N) = \frac{1}{1-k} \times \sum_{\substack{\cap E_w(t) = N \neq \emptyset}} \prod_{1 \le w \le y} m_j(E_w(t)), \tag{1}$$

where *k* is defined as:

$$k = \sum_{\substack{\bigcap E_w(t) = \emptyset}} \prod_{1 \le w \le y} m_j(E_w(t)).$$
<sup>(2)</sup>

According to the Shannon information theory [33], the uncertainty is the highest when  $m_j(E_w(t)) = m_{jw}(N) = 0.5$ . Note, here,  $m_{jw}(N)$  denotes the probabilistic value of a mass function for  $w^{\text{th}}$  event ( $E_w(t)$ ) with the  $j^{\text{th}}$  intersection being normal. If the value of  $m_{jw}(N)$  moves in either direction from 0.5, the uncertainty decreases. Applying the principle of Shannon information theory, the uncertainty associated with  $m_{jw}(N)$  i.e., the probability,  $m_{jw}(N \vee \neg N)$  is defined as:

1

$$m_{jw}(N \vee \neg N) = -m_{jw}(N) log_2 m_{jw}(N) - (1 - m_{iw}(N)) log_2 (1 - m_{iw}(N)).$$
(3)

Since  $m_{jw}(N \land \neg N)$  denotes the null hypothesis, i.e.,  $m_{jw}(N \land \neg N)=0$ ,  $m_{jw}(\neg N)$  is derived as,

$$m_{jw}(\neg N) = 1 - m_{jw}(N) - m_{jw}(N \lor \neg N).$$
 (4)

The upper limit (plausibility) of the *j*<sup>th</sup> intersection being normal is defined as:

$$pl_i(N) = 1 - bel_i(\neg N).$$
(5)

For obtaining the uncertainty value and then the belief value using (3) and (1), respectively, we need to calculate  $m_j(E_w(t))$  for the flow rate, vehicle speed and phase time.

An attacker may attempt to intrude on one or more of the sensors used to collect data for the TMS. To detect whether a sensor has been compromised, we can compare its observed values with the corresponding original (i.e., unaltered) historical values. This process involves the development of probability mass functions, denoted by  $m_j()$ , which are used in the DS theory-based fusion approach defined in (1) and (5). By comparing observed and historical values, our approach enables the identification of abnormal or anomalous sensor behaviour, which can be indicative of a security breach.

# 3.3. Development of the Probability Mass Function

We developed a formula (refer to (6)) to calculate the mass value that identifies an intrusion from a regular traffic signal based on the assumption that the underlying historical data are normally distributed. In the following section, we present an analysis of the validity of such assumptions and converted the data to follow normal distributions when the assumption did not hold true.

# 3.4. Data Conversion into Normal Distribution

As discussed in the previous section, we assumed that the traffic data follow the normal distribution. However, since the traffic data are not normally distributed, we transformed the data so that they follow the normal distribution. For example, the flow rate and vehicle speed distributions before and after normal transformation for Intersection 1 are shown in Figures 2 and 3.







Figure 3. Histograms for vehicle speed original and transformed data.

We applied the BoxCox transformation [34], which can transform the data to a normal distribution. The following equation defines BoxCox transformation.

$$y = \begin{cases} \frac{(x^{\lambda} - 1)}{\lambda} & \text{for } \lambda \neq 0\\ \log(x) & \text{for } \lambda = 0. \end{cases}$$
(6)

Here, *x* and *y* represent data before and after the BoxCox transformation, respectively, and  $\lambda$  is a transformation parameter.

The calculation method for the probability of the observed evidence (e.g., flow rate, vehicle speed, and phase time) developed from the historical data using the probability mass functions is described below.

# 3.5. Probabilities of Observed Evidence for Flow Rate and Vehicle Speed

For an event w and the observed value  $x_w$ , the probability of the evidence can be calculated using (7).

$$m_{j}(x_{w}) = \begin{cases} 1 - \frac{\sqrt{2}}{\sqrt{\pi}} \int_{0}^{z_{w}} e^{-\frac{x^{2}}{2}} dx \text{ if } z_{w} \ge 0\\ 1 - \frac{\sqrt{2}}{\sqrt{\pi}} \int_{z_{w}}^{0} e^{-\frac{x^{2}}{2}} dx \text{ otherwise,} \end{cases}$$
(7)

where  $z_w = (x_w - \mu_w)/\sigma_w$ ,  $x_w = E_w(t)$ , and  $\sigma_w$  and  $\mu_w$  are the standard deviation and mean of the probability mass function, respectively.

### 3.6. Probability of Observed Evidence for Phase Time

The probability of observed phase times was computed. As the phase times observed take values from a limited set, they usually do not follow the normal distribution. Consequently, the probabilities were computed based on the frequency of observed phase times and the relative distance between an individual phase time with the most observed one. In calculating the probabilities, we used the two following rules, i.e., (i) assigning higher probabilities to those phase time values that are more frequently observed, and (ii) assigning higher values to those that are relatively closer to the most-observed value. The following equations capture such probabilities:

$$m_{j}(x_{w}) = \begin{cases} \alpha - \alpha \times \frac{(\min(X) - x_{w})}{\min(X)} \text{ if } x_{w} < \min(X) \\ \alpha \times \frac{(CT - x_{w})}{CT} & \text{ if } x_{w} > \max(X) \\ e^{(\frac{A+B}{2} - 1)} & \text{ if } \min(X) \le x_{w} \le \max(X), \end{cases}$$

$$(8)$$

where

$$A = \frac{f(x_w)}{\max(f(X))} \tag{9}$$

and

$$B = (1 - \frac{|(x_w - argmax(f(X)))|}{max(X) - min(X)}).$$
(10)

Here, *A* and *B* are the two rules described above capturing the frequency of occurrence and the relative distance of an observation from the most frequently observed one. min(X) and max(X) represent the minimum and maximum phase time values observed in the historical data.  $f(x_w)$  and f(X), respectively, represent the frequency of the phase time value  $x_w$  and the frequency distribution of all phase times observed in the historical data *X*. argmax(f(X)) represents the phase time that occurred most in the data set. Finally, *CT* represents the cycle time with a typical value of 180, and  $\alpha$  is a chosen parameter that controls the behaviour of the probability function defined in (8), when the phase time observation falls beyond the minimum and maximum values in the historical data and  $\alpha$  is chosen as 0.4.

### 4. Evaluating the Traffic Signal to Detect Intrusion

In the next step, we evaluated the status of a traffic signal to detect an intrusion in that traffic signal. The standard behaviour profile of a traffic signal was determined using the evaluated status of that traffic signal. Once the value of current events (e.g.,  $E_F(t)$ ,  $E_S(t)$ ,  $E_P(t)$ ) are determined, their probabilities can be calculated as  $m_j(E_F(t))$ ,  $m_j(E_P(t))$ , and  $m_j(E_S(t))$  using (7) and the  $\mu$  and  $\sigma$  of their corresponding probability mass functions. After this, the probability of being N, i.e.,  $bel_j(N)$  defined in (1), needs to be determined. If  $bel_j(N) \ge \Phi$ , the traffic signal of  $j^{\text{th}}$  intersection is considered to be normal, otherwise, it is not normal (intruded). Here,  $\Phi$  is an intuitively-selected threshold that is used in Step 5 of our model (ref to Figure 1). The performance metrics of our proposed methods depend on the value of  $\Phi$ . In an ideal case, the value of  $\Phi$  can be considered 0.5.

### 4.1. Simulation Environment

We used the map of Melbourne CBD and VicRoads' traffic data [35] for five critical intersections and created a simulation environment in SUMO using a popular microscopic traffic model presented in [14] and the Krauss car following model [36,37]. The selected intersections were (i) Lonsdale and Russel Street, (ii) Collins and Kings St, (iii) Elizabeth and Latrobe St, (iv) Collins, and Swanston St, and (v) Flinders and Swanston St Melbourne. For traffic data, we selected the peak-time traffic data from 08:00 a.m. to 10:00 a.m. Monday.

Normal and intrusion scenarios: for normal traffic conditions, the flow rate, vehicle speed, and phase time of an intersection for a particular scenario were derived through our above-mentioned simulation model developed using SUMO. The traffic distributions were initiated with the respective and normal (non-compromised) historical traffic information obtained from the VicRoads online data [30] in our simulation environment. To emulate the current traffic in the simulation, the density, vehicle speed, and phase time of the incoming and outgoing traffic of an intersection of interest were randomly selected from the range of the [minimum, maximum] value of the respective historical data for that day and time period collected from three years (2016–2018) of data available on the VicRoads website. Traffic volumes for the freeways and arterial roads data were taken from [38], signal details for simulation were taken from [39], and traffic signal volume data were taken from [40].

Figures 4 and 5 show the traffic flow of Intersection 1, namely Lonsdale and Russel Street, for its normal and intruded conditions, respectively.



Figure 4. The traffic condition of the simulation environment for the normal scenario.



Figure 5. The traffic condition of the simulation environment for the intruded scenario.

As described in Section 2.1, traffic signals can be the victim of the intrusion. For simulating intrusions to the traffic signals, the flow rate of an intersection and/or average vehicle speed for a particular scenario was changed by intuitively induced phase time and vice versa. The induced average vehicle speed of an intersection was also inserted while phase time and the flow rate were normal. If the intersection is intruded for a very short time (e.g., less than one cycle time), flow rate, vehicle speed, and phase time data will remain within the range of 68% to 95% confidence intervals. If the duration of the intrusion is higher, flow rate, vehicle speed, and phase time will go outside the 95% confidence interval. To consider both cases (e.g., short and long time intrusion), the flow rate, vehicle speed, or phase time were induced in such a way that they remain within 68% to 95% confidence intervals in some cases (Scenario 2 and Scenario 4) and outside 95% confidence intervals of the relevant historical data for the other cases.

We used historical data to observe the current status of a traffic signal for a given point in time. Four different scenarios were created to test 40, 41, 39, 42, and 44 pieces of evidence for Intersection 1, Intersection 2, Intersection 3, Intersection 4, and Intersection 5, respectively. Scenarios 1 to 4 described in Section 4.3 show how different types of evidence (e.g., flow rate, phase time, and vehicle speed) were used. Using the normal historical data taken from the VicRoads website [30], initially, we simulated normal traffic scenarios. We simulated different malicious and abnormal traffic situations. The abnormal situations include incidents, vehicle breakdowns, unusual vehicle stops, and malicious driving behaviour to see the impact of these scenarios on traffic conditions. Note that, in normal traffic conditions, vehicle breakdown creates a traffic jam which reflects the jamming attack. Using Sybil attack, vehicles can be stopped or redirected. Therefore, consideration of unusual vehicle stops is regarded as the impact of a Sybil attack. By injecting false data in GPS or traffic signals, the driving behaviour of a vehicle can be manipulated, representing the false data injection attacks in the situations used in abnormal traffic scenario generation. Abnormal traffic scenarios (Scenario 2 and 4) were created considering the types of attacks mentioned here affecting flow rate, vehicle speed, and phase time of a traffic signal.

The simulation was modified in six different ways to create intruded scenarios. These modifications are described below:

Type 1: Congestion attack scenario

The number of vehicles on the route was falsely increased by modifying the following parameters. This modification would create an incorrect flow rate and cause the traffic controller to miscalculate the average speed. This scenario represents congestion attacks because it falsely increases on-road traffic.

Type 2: False vehicle number injection scenario

By changing the state of the lane area detector, the actual number of vehicles on the detector is overridden, leading to miscalculation of congestion on the cell and disrupting the dynamic adaptation of the traffic light phases.

Type 3: Replay attack scenario

Induction loop state values were replayed at certain intervals and transmitted to the regional traffic controller. This attack modifies flow rate count and average vehicle speed.

Type 4: Sybil attack scenario

The simulation environment is tampered by introducing a multitude of fake vehicles and sensors, which sent erroneous traffic data to the traffic controller system in such a manner that may create congestion on the roadways.

Type 5: False traffic light state injection

A false traffic light state was injected to modify the phase times, creating an impact of false traffic control.

Type 6: Jamming attack scenario

The lane attributes can be changed by transmitting false values or man-in-the-middle attacks. Examples of such attributes include the allowed speed limit, permitted vehicle categories, restricted vehicles, acceptable turns, and lane change permissions. These changes force vehicles to make incorrect turns, travel at varying speeds, and prevent certain vehicles from entering the lane.

The above scenarios consider most attacks that were previously observed in traffic signal intrusions (see Section 2.1).

### 4.2. Performance Metrics

Widely used standard performance metrics such as specificity, sensitivity, overall accuracy, and F-Score were employed to evaluate our model. If the normal (non-intruded) event is detected correctly, it is considered a True Positive (*TP*). Conversely, when an intruded event is detected as normal, it is marked as False Positive (*FP*). When the system is able to detect the intruded event correctly, it is considered a True Negative (*TN*), but when the system detected a normal event as an intruded event, it is considered a False negative (*FN*) value. The accuracy, sensitivity, specificity, and F-Score are defined as follows:

$$Accuracy = \frac{TN + TP}{TP + TN + \mathcal{F}P + \mathcal{F}N};$$
(11)

$$Sensitivity = \frac{TP}{TP + \mathcal{F}N};$$
(12)

$$Specificity = \frac{TN}{TN + \mathcal{F}P};$$
(13)

$$F-Score = 2 \times \frac{Sensitivity \times Precision}{Sensitivity + Precision}.$$
 (14)

### 4.3. Results and Analysis

We used 206 observations for the five intersections for each piece of evidence (FP, FS, PS, and FPS) and scenario. Therefore, the total number of observations we used was  $206 \times 4 \times 4 = 3296$ . These 206 observations were distributed to 40, 41, 39, 42, and 44 observations for Intersections 1 to 5, respectively. As a representative sample, Tables 1–4 show the probabilities of signals being normal (*N*), not normal ( $\neg N$ ), and the uncertainty (*N*,  $\neg N$ ) for Scenarios 1–4 having various flow rates, average speeds, and phase times. Note, Scenarios 1 and 3 were created using the original data collected from VicRoads to emulate normal traffic conditions without intrusion. Scenarios 2 and 4 were created to induce intrusions by using the same data but manipulating a combination of flow rate, phase time, and average vehicle speed.

**Table 1.** Detection results for Scenario 1. In the simulation, all intersections operated in normal conditions. The values that are highlighted in bold represent the combination that produces the best outcome.

	Normal (N)				Not N	Not Normal ( $\neg N$ )				Uncertainty ( $N \lor \neg N$ )			
	FS	FP	PS	FPS	FS	FP	PS	FPS	FS	FP	PS	FPS	
1	0.58	0.65	0.71	0.76	0.3	0.29	0.27	0.16	0.12	0.06	0.02	0.08	
2	0.75	0.58	0.64	0.72	0.23	0.31	0.29	0.17	0.02	0.11	0.07	0.11	
3	0.48	0.52	0.67	0.58	0.39	0.36	0.29	0.21	0.13	0.12	0.04	0.21	
4	0.61	0.61	0.76	0.63	0.31	0.29	0.21	0.25	0.08	0.1	0.03	0.12	
5	0.57	0.52	0.58	0.59	0.32	0.39	0.3	0.22	0.11	0.09	0.12	0.19	

	Normal (N)				Not Normal ( $\neg N$ )				Uncertainty ( $N \lor \neg N$ )			
	FS	FP	PS	FPS	FS	FP	PS	FPS	FS	FP	PS	FPS
1	0.41	0.38	0.24	0.41	0.51	0.53	0.64	0.5	0.08	0.09	0.12	0.09
2	0.32	0.27	0.32	0.38	0.62	0.64	0.57	0.56	0.06	0.09	0.11	0.06
3	0.27	0.48	0.32	0.46	0.66	0.44	0.62	0.43	0.07	0.08	0.06	0.11
4	0.19	0.24	0.21	0.33	0.72	0.69	0.71	0.55	0.09	0.07	0.08	0.12
5	0.23	0.17	0.26	0.28	0.63	0.72	0.62	0.54	0.14	0.11	0.12	0.18

**Table 2.** Detection results for Scenario 2. In the simulation, all intersections were intuitively intruded (not normal). The values that are highlighted in bold represent the combination that produces the best outcome.

**Table 3.** Detection results for Scenario 3. In the simulation, all intersections operated in normal conditions. The values that are highlighted in bold represent the combination that produces the best outcome.

	Normal (N)				Not Normal ( $\neg N$ )				Uncertainty ( $N \lor \neg N$ )			
	FS	FP	PS	FPS	FS	FP	PS	FPS	FS	FP	PS	FPS
1	0.68	0.61	0.59	0.74	0.27	0.33	0.35	0.2	0.05	0.06	0.04	0.06
2	0.42	0.48	0.50	0.51	0.51	0.42	0.51	0.32	0.07	0.1	0.06	0.12
3	0.65	0.58	0.66	0.51	0.30	0.36	0.34	0.47	0.05	0.06	0.06	0.03
4	0.67	0.71	0.65	0.72	0.26	0.20	0.26	0.16	0.04	0.09	0.09	0.13
5	0.65	0.63	0.67	0.69	0.33	0.35	0.30	0.25	0.02	0.02	0.03	0.06

**Table 4.** Detection results for Scenario 4. In the simulation, all intersections were intuitively intruded (not normal). The values that are highlighted in bold represent the combination that produces the best outcome.

	Normal (N)				Not Normal ( $\neg N$ )				Uncertainty ( $N \lor \neg N$ )			
	FS	FP	PS	FPS	FS	FP	PS	FPS	FS	FP	PS	FPS
1	0.20	0.24	0.22	0.22	0.74	0.71	0.65	0.6	0.06	0.05	0.12	0.14
2	0.18	0.16	0.17	0.14	0.71	0.65	0.72	0.70	0.10	0.19	0.11	0.16
3	0.01	0.02	0.02	0.09	0.92	0.91	0.88	0.78	0.08	0.07	0.11	0.13
4	0.23	0.22	0.18	0.27	0.73	0.67	0.72	0.56	0.04	0.11	0.10	0.17
5	0.31	0.26	0.34	0.38	0.53	0.62	0.57	0.40	0.16	0.11	0.09	0.22

We used four different types of combinations for two different observations of an intersection. Four different combinations of two observations are (i) flow rate and phase time (FP), (ii) flow rate and vehicle speed (FS), (iii) phase time and vehicle speed (PS), and (iv) flow rate, phase time, and vehicle speed (FPS).

Tables 1 and 3 present the intrusion detection results and their uncertainty values produced by our system for Scenarios 1 and 3, where no intrusions happened in any of the five intersections. Note, since uncertainty values are shown separately in all tables, throughout the chapter, belief values obtained by (1) denote the results. In contrast, Tables 2 and 4 show the results for Scenarios 2 and 4 where intersections were intruded. Therefore, Scenarios 1 and 3 represent normal intersections, while Scenarios 2 and 4 are for the intruded intersections. The probability values highlighted with bold text represent which combination provides the best result. It also shows the combinations that have the lowest uncertainty.

### 4.3.1. Detection Probability

In the case of intrusion in an intersection, the results produced by combining two pieces of evidence (e.g., FP, FS, PS) provide better detection than the results achieved using all

three pieces of evidence (FPS). For example, in Table 4, our proposed method obtained the maximum detection probability values (e.g., 0.74, 0.72, 0.921, 0.73) for being not normal for four intersections using FS, while for Intersection 5, it (e.g., 0.62) was for FP. Table 4 also shows that the lowest uncertainty values (e.g., 0.06, 0.10, 0.07, 0.04) were obtained for the maximum number of intersections (4/5) using FS. Table 2 also supports a similar trend in the results. The detection probabilities obtained using FPS for Intersection 3 of Scenario 2 (see Table 2) and Intersection 5 of Scenario 4 (refer to Table 4) are 0.43 and 0.40, respectively, which are lower than the selected threshold 0.50, indicating the ineffectiveness of exploiting all three pieces of evidence for capturing intrusion. These results indicate that phase time is a major factor in intrusion detection. If a hacker can intrude on the sensor to change the phase time, it creates more congestion. Phase time impacts the traffic flow and average vehicle speed immediately. In the simulation, Intersection 5 and Intersections 5 and 2, Tables 2 and 4 present the high detection values exhibiting the efficacy of phase time consideration in spotting intrusion.

When the intersection is not intruded, i.e., normal, a combination of all three pieces of evidence (FPS) provides better detection results than the others. These results are above 0.50 for all intersections of the two scenarios. For example, for FS, the probability value for Intersection 3 shown in Table 1 is 0.48, while it is 0.58 for FPS. Table 3 shows that the probability values for Intersection 2 are 0.42, 0.48, and 0.50 for FP, FS, and PS, respectively, compared with 0.51 for FPS. These superior detection outcomes vindicate the use of FPS (three or more pieces of evidence) for the accurate detection of normal traffic conditions. The only loophole of FPS utilisation is that its uncertainty value is higher than that of others but not that high as its maximum value of 0.12. This higher uncertainty value is justified by the fact that, in a normal scenario, the real traffic conditions are dynamic. Traffic conditions may change due to many different reasons, such as different times (peak, off-peak), weather conditions, special events (e.g., road works, sports events), and school time. Flow rate, average vehicle speed, and phase time are affected because of the dynamic characteristics of the traffic conditions.

From the results discussed so far, it is evident that FPS is effective at identifying normal traffic conditions, but not so effective for intruded intersection detection. However, if we use the maximum probabilistic values, highlighted in bold, of an intersection in Tables 1–4, our proposed system is able to detect the correct state (normal or intruded) of all intersections. For example, for intersections being normal, the maximum values for Intersection 3 in Table 1 and Intersection 2 in Table 3 are max (0.48, 0.52, 0.67, 0.58) = 0.67 and max (0.42, 0.48, 0.43, 0.51) = 0.51, respectively. Note, since for both intersections, these two maximum values (0.67 and 0.51) are above 0.50, our proposed system can detect normal traffic conditions accurately.

To show how our proposed IDS works to detect both traffic conditions for each intersection, we calculated the average value of the probabilities for both scenarios. Figures 6 and 7 show these average detection results for the normal and intruded traffic conditions, respectively. In Figures 6 and 7, for each intersection, there are 12 bars. The first four bars represent the probability of an intersection being normal, bars five to eight denote the probability of an intersection being not normal, and the last four bars show the uncertainty values. For the normal traffic conditions, as with the results shown in Tables 1 and 3, for FS, the detection probabilities shown in Figure 6 are higher and above or equal to 0.62 for all interactions except Intersection 3. For these intersections for FSP, Figure 6 also shows higher uncertainty values. However, for the intruded traffic conditions, the probability values for FSP for all intersections are less than those of the others having higher uncertainty values except for Intersection 4.



Figure 6. Average detection probability for normal intersections.



Figure 7. Average detection probability for intruded intersections.

### 4.3.2. Class Separability

As we know, the wider separation gap between the value of two decisive parameters makes the system robust and decisions more accurate. For this reason, to show the robustness of our proposed IDS in deciding whether an intersection is normal or not normal, we calculated the separation gap between the average probability values for all pieces of evidence being normal or not normal for any particular intersection.

The separation band of the values of an intersection being normal or intruded is shown in Figures 8 and 9, respectively. The highest gap calculated is for Intersection 4, shown in Figure 8, which has a probability of being not normal of 0.76, and of being normal of 0.27. So, the gap is 0.59. The lowest gap is for Intersection 5, shown in Figure 9. The probability of being normal is 0.615, and not normal is 0.38, and thus the lowest gap is 0.235. The wide separation gap ranging from 0.235 to 0.59 vindicates that our system can conveniently differentiate the normal and intruded intersections.



Figure 8. Separation gap between the probability of intersection being normal.



Figure 9. Separation gap between the probability of intersection being intruded.

4.3.3. Detection Performance

We demonstrated the performance of the proposed model in terms of its ability to detect intruded and non-intruded scenarios accurately. For this, we calculated the value of four performance metrics—sensitivity, specificity, accuracy, and F1-Score —using Equations (13) and (14); this is shown in Table 5.

**Table 5.** Detection results in terms of standard performance metrics. Here, TP = (True Positive), TN = (True Negative),  $\mathcal{F}P = \text{False Positive}$ ,  $\mathcal{F}N = \text{False Negative}$ , Sen. = Sensitivity, Spec. = Specificity, Acc. = Accuracy, and F1 = F1-Score.

		TP	TN	$\mathcal{F}P$	$\mathcal{F}N$	Sen.	Spec.	Acc.	F1
	1	1960	678	122	536	0.79	0.85	0.80	0.82
	2	2052	306	194	444	0.82	0.61	0.79	0.70
FP	3	2316	664	136	380	0.86	0.83	0.85	0.84
	4	2157	513	287	439	0.83	0.64	0.79	0.72
	5	2324	505	295	572	0.80	0.63	0.77	0.71
	1	2352	619	181	414	0.85	0.77	0.83	0.81
	2	2025	578	222	471	0.81	0.72	0.79	0.76
PS	3	2435	626	174	382	0.86	0.78	0.85	0.82
	4	2187	606	194	309	0.88	0.76	0.85	0.81
	5	2343	582	218	453	0.84	0.73	0.81	0.78

		TP	TN	$\mathcal{F}P$	$\mathcal{F}N$	Sen.	Spec.	Acc.	F1
	1	2074	577	223	322	0.87	0.72	0.83	0.79
	2	2295	612	188	401	0.85	0.77	0.83	0.81
FS	3	2377	613	187	512	0.82	0.77	0.81	0.79
	4	1866	589	211	430	0.81	0.74	0.79	0.77
	5	2203	613	187	393	0.85	0.77	0.83	0.81
	1	2126	458	342	612	0.78	0.57	0.73	0.66
	2	2052	473	327	444	0.82	0.59	0.77	0.69
FPS	3	2352	466	334	472	0.83	0.58	0.78	0.69
	4	1826	413	387	417	0.81	0.52	0.74	0.63
	5	2192	496	304	452	0.83	0.62	0.78	0.71
Overall						0.82	0.71	0.79	0.80

Table 5. Cont.

Table 5 displays the performance metrics of different models based on the combination of input features (flow rate, phase time, and vehicle speed). The performance of each model was evaluated using True Positive, True Negative, False Positive, False Negative, sensitivity, specificity, accuracy, and F1-Score. Five different instances (1 to 5) are reported for each model, possibly indicating different test sets or cross-validation results.

1. Flow rate and phase time:

3.

4.

The model utilising flow rate and phase time as features has sensitivity values ranging from 0.79 to 0.86, specificity values between 0.61 and 0.83, accuracy values varying from 0.77 to 0.85, and F1-Scores ranging from 0.70 to 0.84. This model seems to have a relatively good overall performance with varying levels of specificity.

 Phase time and vehicle speed: This model, based on phase time and vehicle speed, shows sensitivity values between 0.81 and 0.88, specificity values ranging from 0.72 to 0.78, accuracy values varying from 0.79 to 0.85, and F1-Scores ranging from 0.76 to 0.82. The performance of this model is consistent and generally good across all instances.

Flow rate and vehicle speed: For the model using flow rate and vehicle speed as features, sensitivity values range from 0.81 to 0.87, specificity values are between 0.72 and 0.77, accuracy values vary from 0.79 to 0.83, and F1-Scores range from 0.77 to 0.81. This model demonstrates a fairly consistent and good performance across all instances, with a slightly lower specificity compared to the phase time and vehicle speed model.

Flow rate, phase time, and vehicle speed:
The model that includes all three features—flow rate, phase time, and vehicle speed—has sensitivity values ranging from 0.78 to 0.83, specificity values between 0.52 and 0.62, accuracy values varying from 0.73 to 0.78, and F1-Scores ranging from 0.63 to 0.71. This model shows a drop in performance, especially in specificity, when compared to the other models.

The models with the best performance are those that utilise two features: phase time and vehicle speed or flow rate and vehicle speed. The phase time and vehicle speed model shows a slightly better performance than the flow rate and vehicle speed model, with higher specificity values. The model using all three features (flow rate, phase time, and vehicle speed) exhibits the lowest performance, especially in specificity. Based on these findings, it is recommended to use the phase time and vehicle speed model or the flow rate and vehicle speed model for further analysis or deployment. Our system is able to detect most of the normal and intruded traffic conditions used in our simulation successfully. Due to the dynamic characteristics, the traffic condition deviates highly from the ideal condition. These dynamic characteristics cause some False Positives and False Negatives. The results presented in Table 5 show that none of the pieces of evidence achieve a superior performance in terms of all metrics. This is because, as mentioned before, there are some situations in which our system could not detect normal traffic conditions accurately.

# 5. Conclusions

In this paper, we introduced a technique to detect intrusion at the traffic signal of an ITS. Our technique is based on the real-time observation of traffic parameters, namely, traffic flow, average vehicle speed, phase time of the signal, and their historical values. Using the past and currently-observed values, probabilistic estimation of those parameters being normal or abnormal was derived using the DS theory. We also used an approach based on Shannon's entropy to incorporate the uncertainty of observed data in the detection system. To validate the efficacy of the proposed IDS, simulation scenarios were built using the SUMO platform and the real road network of Melbourne CBD, utilising the actual data from road transport authority on traffic flow, phase time, and vehicle speed. Intrusion scenarios were created by intentional perturbation of those traffic parameters and the proposed system's capability to identify traffic signal intrusion was assessed in terms of the widely used metrics of detection accuracy, sensitivity, specificity, and F1-Score. The proposed IDS demonstrated an overall accuracy of 79.3% for intruded traffic conditions. Further investigation into the behaviour of the system showed that detection fails if the intrusion is very short-lived in the range of one to two cycles only. This is because such short intrusion fails to produce enough impact in the traffic system to cause a significant deviation from normal data.

The next-generation ITS will be highly complex, comprising autonomous and semiautonomous vehicles, intelligent sensors connected wirelessly to TMS infrastructure, and all requiring ultra-low latency interactions among themselves and with road-side infrastructure. All these expose ITS to new attacks and vulnerabilities. Future work will focus on improving the detection of intrusion and types of intrusion.

**Author Contributions:** Conceptualization, A.C. and G.K.; Software, G.K.; Validation, A.C.; Formal analysis, A.C., G.K., J.K. and R.D.; Investigation, A.C. and R.D.; Writing—original draft, A.C., G.K. and S.H.S.N.; Writing—review & editing, A.C., J.K., R.D. and S.H.S.N.; Visualization, J.K. and S.H.S.N.; Supervision, G.K. and J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

**Data Availability Statement:** Publicly available datasets were analyzed in this study. This data can be found here: [https://vicroadsopendata-vicroadsmaps.opendata.arcgis.com/].

Conflicts of Interest: The authors declare no conflict of interest.

# References

- Salih, K.O.M.; Rashid, T.A.; Radovanovic, D.; Bacanin, N. A comprehensive survey on the Internet of Things with the industrial marketplace. *Sensors* 2022, 22, 730. [CrossRef] [PubMed]
- Chowdhury, A. Priority based and secured traffic management system for emergency vehicle using IoT. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016; pp. 1–6.
- Cafiso, S.; Di Graziano, A.; Giuffrè, T.; Pappalardo, G.; Severino, A. Managed Lane as Strategy for Traffic Flow and Safety: A Case Study of Catania Ring Road. Sustainability 2022, 14, 2915. [CrossRef]
- Ning, Z.; Zhang, F.; Remias, S. Understanding the security of traffic signal infrastructure. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Gothenburg, Sweden, 19–20 June 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 154–174.

- Li, Z.; Jin, D.; Hannon, C.; Shahidehpour, M.; Wang, J. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. *IET Cyber-Phys. Syst. Theory Appl.* 2016, 1, 60–69. [CrossRef]
- Feng, Y.; Huang, S.; Chen, Q.A.; Liu, H.X.; Mao, Z.M. Vulnerability of traffic control system under cyber attacks using falsified data. In Proceedings of the 97th Annual Meeting of the Transportation Research Board, Washington, DC, USA, 7–11 January 2018.
- 7. Wei, Q.; Yang, B. Adaptable vehicle detection and speed estimation for changeable urban traffic with anisotropic magnetoresistive sensors. *IEEE Sens. J.* 2017, 17, 2021–2028. [CrossRef]
- 8. Zhang, X.; Wang, D. Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain. *IEEE Access* **2019**, *7*, 97281–97295. [CrossRef]
- Perrine, K.A.; Levin, M.W.; Yahia, C.N.; Duell, M.; Boyles, S.D. Implications of traffic signal cybersecurity on potential deliberate traffic disruptions. *Transp. Res. Part A Policy Pract.* 2019, 120, 58–70. [CrossRef]
- 10. Turner, G.; Chen, G.; Zhang, Y. A Visual Analytics Approach for Anomaly Detection from a Novel Traffic Light Data. *Electron. Imaging* **2021**, 2021, 330–331. [CrossRef]
- Xiang, Y.; Niu, W.; Tong, E.; Li, Y.; Jia, B.; Wu, Y.; Liu, J.; Chang, L.; Li, G. Congestion attack detection in intelligent traffic signal system: Combining empirical and analytical methods. *Secur. Commun. Netw.* 2021, 2021, 1–17. [CrossRef]
- 12. Li, Y.; Xiang, Y.; Tong, E.; Niu, W.; Jia, B.; Li, L.; Liu, J.; Han, Z. An empirical study on gan-based traffic congestion attack analysis: A visualized method. *Wirel. Commun. Mob. Comput.* **2020**, 2020, 1–14. [CrossRef]
- Chowdhury, A.; Karmakar, G.; Kamruzzaman, J.; Saha, T. Detecting Intrusion in the Traffic Signals of an Intelligent Traffic System. In Proceedings of the International Conference on Information and Communications Security, Lille, France, 29–31 October 2018; Springer: Cham, Switzerland, 2018; pp. 696–707.
- 14. Han, G.H.; Chen, X.R.; Yu, Y.; Li, Y.Q. A study of microscopic traffic simulation based on sumo platform. *Comput. Eng. Sci.* 2012, 34, 195–198.
- 15. Zhu, L.; Yu, F.R.; Wang, Y.; Ning, B.; Tang, T. Big data analytics in intelligent transportation systems: A survey. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 383–398. [CrossRef]
- Gonçalves, F.; Ribeiro, B.; Gama, O.; Santos, A.; Costa, A.; Dias, B.; Macedo, J.; Nicolau, M.J. A systematic review on intelligent intrusion detection systems for VANETs. In Proceedings of the 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 28–30 October 2019; pp. 1–10.
- Gibbs, S. Ransomware Attack on San Francisco Public Transit Gives Everyone a Free Ride. 2016. Available online: https: //www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware (accessed on 12 March 2023).
- 18. Perallos, A.; Hernandez-Jayo, U.; Zuazola, I.J.G.; Onieva, E. Intelligent Transport Systems: Technologies and Applications; John Wiley & Sons: Hoboken, NJ, USA, 2015.
- Li, W.; Nejad, M.; Zhang, R. A blockchain-based architecture for traffic signal control systems. In Proceedings of the 2019 IEEE International Congress on Internet of Things (ICIOT), Milan, Italy, 8–13 July 2019; pp. 33–40.
- Chen, Q.A.; Yin, Y.; Feng, Y.; Mao, Z.M.; Liu, H.X. Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. In Proceedings of the NDSS, San Diego, CA, USA, 18–21 February 2018.
- Wang, X.; Xiang, Y.; Niu, W.; Tong, E.; Chen, Q.A.; Li, G.; Liu, J.; Li, L. Constructing Optimal Sparse Decision Tree for Analying I-SIG System Attack. In Proceedings of the 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Exeter, UK, 17–19 December 2020; pp. 321–328.
- Pretorius, B.; van Niekerk, B. IIoT Security: Do I Really Need a Firewall for my Train? In Proceedings of the ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019, Stellenbosch, South Africa, 28 February–1 March 2019; Academic Conferences and Publishing Limited: Montreal, QC, Canada, 2019; p. 338.
- Naveed, Q.N.; Alqahtani, H.; Khan, R.U.; Almakdi, S.; Alshehri, M.; Abdul Rasheed, M.A. An intelligent traffic surveillance system using integrated wireless sensor network and improved phase timing optimization. *Sensors* 2022, 22, 3333. [CrossRef] [PubMed]
- Xiang, Y.; Chen, T.; Li, Y.; Tian, Y.; Niu, W.; Tong, E.; Liu, J.; Jia, B.; Wu, Y.; Huang, X. Predicting Congestion Attack of Variable Spoofing Frequency for Reliable Traffic Signal System. In Proceedings of the Security and Privacy in New Computing Environments: 4th EAI International Conference, SPNCE 2021, Virtual Event, 10–11 December 2021; Springer: Berlin/Heidelberg, Germany, 2022; pp. 219–237.
- Jiang, N. Optimal signal design for mixed equilibrium networks with autonomous and regular vehicles. J. Adv. Transp. 2017, 2017, 5649823. [CrossRef]
- Bhatnagar, S.; Guo, R.; McCabe, K.; McCluskey, T.L.; Scala, E.; Vallati, M. Leveraging Artificial Intelligence for Simulating Traffic Signal Strategies. In Proceedings of the 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC), Macau, China, 8–12 October 2022; pp. 607–612.
- 27. Wang, H.; Zhu, M.; Hong, W.; Wang, C.; Tao, G.; Wang, Y. Optimizing signal timing control for large urban traffic networks using an adaptive linear quadratic regulator control strategy. *IEEE Trans. Intell. Transp. Syst.* **2020**, *23*, 333–343. [CrossRef]
- Chowdhury, A.; Karmakar, G.; Kamruzzaman, J.; Jolfaei, A.; Das, R. Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access* 2020, *8*, 207308–207342. [CrossRef]

- Javaid, S.; Sufian, A.; Pervaiz, S.; Tanveer, M. Smart traffic management system using Internet of Things. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 11–14 February 2018; pp. 393–398.
- VicRoads. VicRoads Traffic Data. 2019. Available online: https://discover.data.vic.gov.au/dataset/traffic-volume (accessed on 20 February 2023).
- Chowdhury, A.; Karmakar, G.; Kamruzzaman, J.; Islam, S. Trustworthiness of self-driving vehicles for intelligent transportation systems in industry applications. *IEEE Trans. Ind. Inform.* 2020, 17, 961–970. [CrossRef]
- Wu, Y.; Meng, F.; Wang, G.; Yi, P. A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–7.
- 33. Rényi, A. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics;* University of California Press: Berkeley, CA, USA, 1961; pp. 547–561.
- Atkinson, A.C.; Riani, M.; Corbellini, A. The Box–Cox Transformation: Review and Extensions. *Stat. Sci.* 2021, 36, 239–255. [CrossRef]
- Krajzewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. Recent development and applications of SUMO-Simulation of Urban MObility. Int. J. Adv. Syst. Meas. 2012, 5, 128–138.
- Krauß, S. Microscopic Modeling of Traffic Flow: Investigation of Collision Free Vehicle Dynamics. Ph.D. Thesis, Forschungszentrum fuer Luft- und Raumfahrt (DLR), Köln, Germany, 1998.
- Song, J.; Wu, Y.; Xu, Z.; Lin, X. Research on car-following model based on SUMO. In Proceedings of the 7th IEEE/International Conference on Advanced Infocomm Technology, Fuzhou, China, 14–16 November 2014; pp. 47–55.
- VicRoads. Traffic Volume. 2023. Available online: https://vicroadsopendata-vicroadsmaps.opendata.arcgis.com/datasets/ vicroadsmaps::traffic-volume/about (accessed on 12 March 2023).
- VicRoads. Traffic Lights. 2023. Available online: https://vicroadsopendata-vicroadsmaps.opendata.arcgis.com/datasets/ vicroadsmaps::traffic-lights/about (accessed on 12 March 2023).
- VicRoads. Traffic Signal Volume Data. 2023. Available online: https://discover.data.vic.gov.au/dataset/traffic-signal-volumedata (accessed on 12 March 2023).

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.